Universidad Nacional "Pedro Ruiz Gallo"

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO Y GESTION, MEDIANTE EL USO DE VPNs, PARA OPTIMIZAR EL SERVICIO DE SOPORTE EN LOS SISTEMA DE VIDEO VIGILANCIA IMPLEMENTADOS POR LA EMPRESA NETKROM TECHNOLOGIES.

TESIS

PARA OPTAR EL TÍTULO PROFESIONAL DE
INGENIERO ELECTRÓNICO

ELABORADO POR:

Br. PUSE HUANGAL, RONNY OMAR
Br. RUIZ LA TORRE, MARY ELSA

ASESOR:

Ing. OBLITAS VERA, CARLOS LEONARDO

LAMBAYEQUE - PERÚ
2015

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO Y GESTIÓN, MEDIANTE EL USO DE VPNs, PARA OPTIMIZAR EL SERVICIO DE SOPORTE EN LOS SISTEMA DE VIDEO VIGILANCIA IMPLEMENTADOS POR LA EMPRESA NETKROM TECHNOLOGIES.

Para optar por el Título Profesional de Ingeniero Electrónico,

ELABORADO POR:

Br. Puse Huangal, Ronny Omar

Br. Ruiz La Torre, Mary Elsa

ASESOR:

Ing. Oblitas Vera, Carlos Leonardo

LAMBAYEQUE – PERU

2015

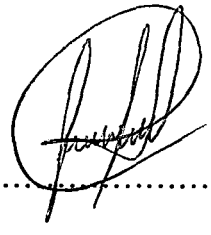
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO Y GESTIÓN, MEDIANTE EL USO DE VPNs, PARA OPTIMIZAR EL SERVICIO DE SOPORTE EN LOS SISTEMA DE VIDEO VIGILANCIA IMPLEMENTADOS POR LA EMPRESA NETKROM TECHNOLOGIES.

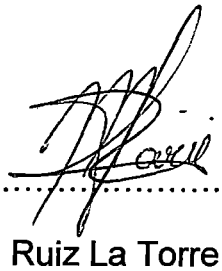
Elaborado por los bachilleres:



.....

Br. Puse Huangal, Ronny Omar

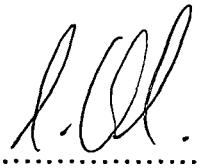
Tesista



.....

Br. Ruiz La Torre, Mary Elsa

Tesista



.....

Ing. Carlos Leonardo Oblitas Vera

Asesor

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO Y GESTIÓN, MEDIANTE EL USO DE VPNs, PARA OPTIMIZAR EL SERVICIO DE SOPORTE EN LOS SISTEMA DE VIDEO VIGILANCIA IMPLEMENTADOS POR LA EMPRESA NETKROM TECHNOLOGIES.

Aprobado por los miembros de jurado:

.....

Ing. Oscar Ucchelly Romero Cortez
Vocal

.....

Ing. Francisco Segura Altamirano
Secretario

.....

Ing. Hugo Javier Chiclayo Padilla

Presidente

DEDICATORIA

Esta tesis se la dedico:

A mis padres Hermel Arminder Puse Ramos y María Petronila Huangal Verastegui quienes me han apoyado para poder llegar a esta instancia de mis estudios, ya que ellos han estado siempre presentes para apoyarme moral y psicológicamente.

A mis Hermanas Yessenia y Melissa quienes son para mí un ejemplo a seguir por su perseverancia y tenacidad.

A mi novia Mary con quien realizamos este trabajo y por todo su apoyo incondicional.

Ronny

DEDICATORIA

Dedico el presente trabajo a Doña Elza Flor La Torre Salazar y Don Pedro Elmer Ruiz Hernández mis padres, quienes han sido para mí un ejemplo de esfuerzo y lucha, y los que han logrado formarme en valores y llegar a esta etapa de mi vida.

A mi mamá Zenaida y mi papá Isidoro, mis abuelos, quienes me han llenado de amor y estuvieron pendientes de mí durante toda mi estadía en la universidad.

A mi novio Ronny, con quien decidimos emprender juntos este camino y dejar constancia de el con este trabajo.

Mary

AGRADECIMIENTO

Agradecemos a Dios, por darnos la vida y la voluntad para finalizar con este proyecto.

A nuestras familias por su constante apoyo y comprensión para lograr que concluyamos con esta etapa de nuestra vida.

Al Ingeniero Carlos Oblitas Vera, nuestro asesor, quien desinteresadamente compartió sus conocimientos y experiencia laboral para apoyarnos en la construcción de este trabajo.

Y finalmente nuestro especial agradecimiento al Ingeniero Romy Monteza, Jefe del Área de Soporte "NOC" de la Empresa Netkrom Technologies quien nos brindó todo su apoyo durante el desarrollo de este proyecto.

RESUMEN

En el presente trabajo se detalla el diseño e implementación de un sistema de monitoreo y gestión para las redes implementadas por la empresa Netkrom Technologies.

Para lograr la interconexión de todas las redes con la estación de la empresa se utilizaron dispositivos Mikrotik en los cuales configuramos VPNs mediante el uso del protocolo PPTP.

Mediante la habilitación del protocolo SNMP en todos los dispositivos de la red se logró gestionar y monitorear dichos dispositivos desde un servidor al cual se le instaló el software The DUDE, y así este cumpla la función de NMS.

Dicho NMS nos permitió crear Mapas de Red, monitorear y graficar parámetros determinados, configurar alarmas, enviar notificaciones, llevar un historial de eventos y tener acceso remoto a los dispositivos de la red.

ABSTRACT

The present paper detailed the design and implementation of a monitoring and management system, for networks that were implemented by the company Netkrom Technologies.

To achieve the interconnection of all networks with the main station of the company, we used Mikrotik devices in which we configured VPNs using the PPTP protocol.

By enabling SNMP protocol on all network devices, we can manage and monitor those devices, from a server to which you installed the software The DUDE, so this fulfills the function of NMS.

This NMS allowed us to create network maps, monitoring and plot certain parameters, set alarms, send notifications, keeping a record of events and have remote access to network devices.

ABREVIATURAS

TIC: Tecnología de la Información y Comunicación

SLA: Service-level agreement (Acuerdo de Nivel de Servicio)

VPN: Virtual Private Network (Red Privada Virtual)

NMS: Network Management Station (Estaciones Gestoras de Red)

NMA: Network Management Application (Aplicación gestora de red)

MN: Managed Nodes (Nodos gestionados)

MIB: Management Information Base (Bases de Información de Gestión)

OSI: OpenSystem Interconnection (modelo de interconexión de sistemas abiertos)

ISO: International Organization for Standardization (Organización Internacional de Normalización)

CMIS: Common Management Information Service (Servicio de administración de información común)

CMIP: Common Management Information Protocols (Protocolo de administración de información común)

TCP: Transmission Control Protocol (Protocolo de control de transmisión)

IP: Internet Protocol (Protocolo de Internet)

CMOT: Common Management Over TCP/IP (administración de información común sobre TCP/IP)

SNMP: Simple Network Management Protocol (Protocolo Simple de Administración de Red)

SNMPv2: Simple Network Management Protocol version 2 (Protocolo Simple de Administración de Red versión 2)

SNMPv3: Simple Network Management Protocol version 3 (Protocolo Simple de Administración de Red versión 3)

MD5: Message-Digest Algorithm 5 (Algoritmo de Resumen del Mensaje 5)

TMN: Telecommunications Management Network (Gestión de Redes de Telecomunicaciones)

ICMP: Internet Control Message Protocol (Protocolo de Mensajes de Control de Internet)

UDP: User Datagram Protocol (Protocolo de datagrama de usuario)

EGP: Exterior Gateway Protocol (Protocolo de salida exterior)

ITU-T: Telecommunication Standarization Sector of the International Telecommunications Union (Sector de Normalización de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones)

RFC: Request for Comments

SMI: Structure of Management Information (Estructura de la Información de Gestión)

OID: Object Identifiers (Identificadores de Objetos)

ASN.1: Abstract Syntax Notation One (Notación Sintáctica Abstracta 1)

BER: Basic Encryption Rule (Regla Básica de Encriptación)

SGMP: Simple Gateway Monitoring Protocol (Protocolo simple de monitoreo de Gateway)

PDU: Protocol Data Unit (Unidad de datos de protocolo)

LAN: Local Area Network (Red de área local)

WAN: Wide Area Network (Red de área amplia)

ISP: Internet Service Provider (Proveedor de Servicios de Internet)

PPTP: Point-to-Point Tunneling Protocol (Protocolo de Túnel Punto a Punto)

PPP: Point-to-Point Protocol (Protocolo punto a punto)

NAS: Network Access Server (Servidor de Acceso a Red)

IETF: Internet Engineering Task Force (Grupo de Trabajo de Ingeniería de Internet)

GRE: Generic Routing Encapsulation (Encapsulación Genérica para Ruteo)

PAC: PPTP Access Concentrator (Concentrador de Acceso PPTP)

PSTN: Public Switched Telephone Network (Red Telefónica Pública Conmutada)

ISDN/RDSI: Integrated Services for Digital Network / Red Digital de Servicios Integrados

PNS: PPTP Network Server (Servidor de Red PPTP)

FEP: Front End Processo (Procesador Final Frontal)

LCP: Link Control Protocol (protocolo de control de enlace)

NCP: Network Control Protocol (Protocolos PPP de control de red)

CHAP: Challenge Handshake Authentication Protocol (Protocolo de Autenticación por desafío mutuo)

MS-CHAP: Microsoft Challenge Handshake Authentication Protocol (Versión de Microsoft del Protocolo de Autenticación por desafío mutuo)

PAP: Password Authentication Protocol (Protocolo de autenticación de contraseña)

EAP: Extensible Authentication Protocol (Protocolo de autenticación extensible)

EAP-TLS: Extensible Authentication Protocol-Transport Layer Security (Protocolo de autenticación extensible - seguridad de nivel de transporte)

PKI: Public Key Infrastructure (Infraestructura de Clave Pública)

MPPE: Microsoft Point to Point Encryption (Cifrado punto a punto de Microsoft)

RSA: Rivest-Shamir-Adleman

RC4: River Cipher 4

IANA: Internet Assigned Numbers Authority (Entidad que supervisa la asignación global de direcciones IP)

CCM: Centro de Control y Monitoreo

CCTV: Closed Circuit Televisión (Circuito Cerrado de Televisión)

CPU: Central Processing Unit (Unidad Central de Procesamiento)

SSH: Secure Shell (Intérprete de órdenes segura)

PTZ: Pan / Tilt / Zoom (Paneo/ Inclinación/ Ampliación)

INDICE GENERAL

LISTA DE FIGURAS

TABLAS

INTRODUCCIÓN

Netkrom, es una empresa especializada en soluciones y Productos de telecomunicaciones, TIC[1] y seguridad electrónica, promueve y utiliza la tecnología inalámbrica en casi todas sus soluciones aplicadas a los sectores corporativos, gobierno, Municipalidades, educación, entre otros.

Entre sus principales proyectos se puede mencionar, el que consistió en dotar a las Municipalidades de Lima tales como: El Rímac, El Agustino. San Borja, San Isidro, S. J. Lurigancho, San Miguel, Surquillo, ATE y algunas provincias: Arequipa, Puno, Piura, Cajamarca, Cusco y Apurímac con un sistema de video vigilancia inalámbrico conformado por una red de cámaras de vigilancia ubicadas en las zonas de mayor tránsito y comercio de cada distrito.

Esta red de cámaras utiliza un medio de comunicación inalámbrico de banda ancha capaz de transmitir en tiempo real todas las ocurrencias y eventos que estas registren a su centro de control y monitoreo el cual remotamente controla a cada una de las cámaras así como realizar la grabación de todos sus eventos.

Dentro del proyecto de implementación, Netkrom incluye un servicio de soporte SLA[2] 24x7 por periodos que van desde los 2 a 3 años dependiendo del contrato del cliente, este servicio debe garantizar el correcto funcionamiento del sistema, dando solución en un tiempo menor a 12 horas a problemas como: configuración de cámaras, configuración de enlaces y fallas de hardware, aclarando que los problemas de suministro eléctrico no se encuentran dentro de las responsabilidades de la empresa.

[1] TIC: Tecnología de la Información y Comunicación

[2] SLA: Service-level agreement (Acuerdo de Nivel de Servicio)

Pero Netkrom no tiene ningún control sobre los centros de monitoreo y cuando se presenta alguna de estas averías, estos son informados por los operadores de dichos centros, mediante llamadas o correos. Este escenario promueve el tener una errónea información de lo que acontece realmente, prestándose al desplazamiento innecesario de personal o muchas veces sin el materia adecuado para el tratamiento del problema, ya que la mayoría de estos problemas pueden ser resueltos remotamente u otros no son parte del servicio establecido, lo cual genera un mayor gasto, además de retrasar la atención del problema, dejándolos sin servicio un mayor tiempo, y con ello dañando la imagen de la empresa.

Por ello el presente trabajo tiene como finalidad la implementación de un centro de monitoreo y gestión de los servicios brindados por la empresa que garantice el correcto funcionamiento de sus enlaces y brinde un soporte correctivo – preventivo más eficiente de ellos, logrando así que averías de: configuración de cámaras, configuración de enlaces y fallas de hardware sean detectadas y solucionadas dentro de los SLA establecidos. El monitoreo y gestión se dará desde las instalaciones de la empresa Netkrom de forma remota vía internet mediante el uso de VPNs[3], para garantizar la seguridad de la información.

[3] VPN: Virtual Private Network (Red Privada Virtual)

OBJETIVOS

Objetivo General

Diseñar e implementar un sistema de monitoreo y gestión, mediante el uso de VPNs, para optimizar el servicio de soporte en los sistema de video vigilancia implementados por la empresa Netkrom Technologies.

Objetivos Específicos	Tareas
Recolección y Análisis de Información de las redes instaladas	• Recopilación de topologías de Red. • Realizar un estudio de los problemas presentados con mayor frecuencia dentro de los sistemas de video (Configuración, falta de fluido eléctrico, averías por hardware, etc.)
Diseñar e implementar un centro de datos donde concentraremos toda la información y se monitoreará y gestionará los enlaces en el área de soporte de la empresa Netkrom Technologies	• Instalación de un router Mikrotik. • Creación de una VPN Server. • Realizar la interconexión entre las VPNs creadas. • Instalación de PCs y Pantallas de Monitoreo • Instalación del NMS Cliente en las PCs del personal a cargo de la gestión y monitoreo
Establecer el canal seguro por el cual viajara la información de los enlaces, desde los clientes al centro de datos	• Evaluación del ancho de banda requerido. • Creación de una VPN cliente en cada una de las instituciones en las cuales NETKROM tiene implementados enlaces inalámbricos para sus sistemas de video-vigilancia. • Creación de los accesos al personal autorizado, Considerando permisos por niveles.
Implementar un sistema de almacenamiento y gestión de los datos obtenidos acerca del estado de la red en los centros de control de los clientes.	• Implementar y configurar routers Mikrotik, en cada uno de los centros de monitoreo, habilitar el protocolo de SNTP en los dispositivos que componen la red.
Permitir el Monitoreo de la Red de Radio Enlaces existentes en los diferentes clientes de la empresa Netkrom.	• Establecer el esquema de monitoreo, configurar los servicios que se desean monitorear.
Optimizar los recursos humanos empleados en la atención de problemas para la reducción de costos y mejorar los tiempos de Respuesta ante averías	capacitar al personal en el uso del sistema, así se lograra atender las averías en el menor tiempo posible logrando obtener un diagnóstico de la avería sin necesidad de movilizar personal a sitio

Tabla 1 Objetivos Específicos y Tareas

CAPÍTULO I

GESTIÓN Y MONITOREO DE RED

CAPÍTULO I

GESTIÓN Y MONITOREO DE RED

1.1 Gestión de Redes.

1.1.1 Introducción

La existencia de dispositivos de comunicación dispersos en distintas áreas geográficas sobre los que se implementan e interconectan todo tipo de redes y enlaces de comunicación con el fin de acceder a servicios avanzados de telecomunicaciones nos obliga a disponer de sistemas para la configuración, supervisión y diagnóstico de todos estos dispositivos de manera remota. Y es por ello que la gestión de redes se ha vuelto un tema de vital importancia en el mundo de las telecomunicaciones. Pero, ¿qué es la gestión de redes?

Antoni Barba (1999) la define como la planificación, la organización, la supervisión y el control de elementos de comunicaciones para garantizar un adecuado nivel de servicio, y de acuerdo con un determinado coste.

La gestión de red tiene como objetivos principales mejorar la disponibilidad y el rendimiento de los elementos del sistema, así como incrementar su efectividad. [1]

La gestión de red se basa en tres componentes básicos:

- Componente Organizacional: Define la estructura para el proceso de gestión y la estrategia apropiada para llevarlo a cabo de acuerdo con las necesidades del negocio.
- Componente Técnico: Define las herramientas a usar para realizar la función de gestión, y su implantación en la infraestructura.
- Componente Funcional: Define las funciones de gestión que el componente organizacional debe ejecutar utilizando las herramientas de gestión[2]

1 Gestión de Red- Antoni Barba Martí- Edición UCP 1999, Página 15

2 Gestión de Red- Paco Orozco - 2010, Página 5

1.1.2 El Paradigma Gestor – Agente

La mayoría de sistemas de gestión de red se basan en el paradigma Gestor-Agente, siendo este el modelo cliente/servidor tradicional, compuesto por estaciones gestoras y agentes actuando junto con un protocolo de red.[3]

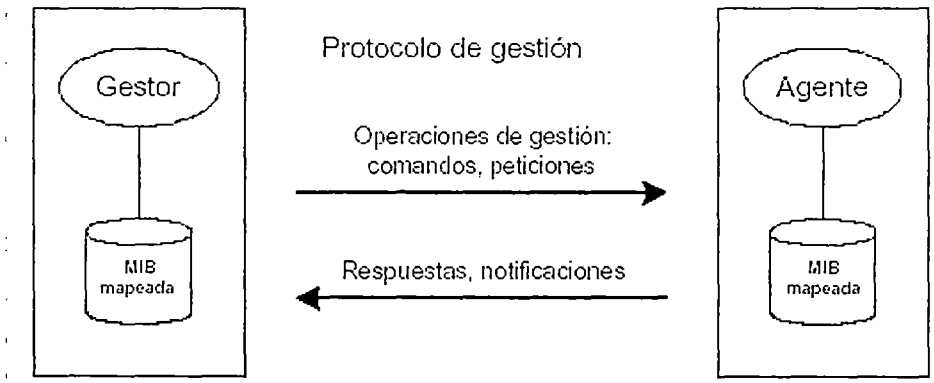


Ilustración 1 Paradigma Gestor-Agente

- Gestores: Estaciones Gestoras (NMS, Network Management Station), nodo en el que se ejecuta la aplicación gestora de red (NMA, Network Management Application). Interactúa con los operadores humanos, son los clientes que piden información a los agentes.
- Agentes: Nodos gestionados (MN, Managed Nodes), elementos de red como host, puentes, router, gateway, etc. En estos reside el agente gestor encargado de llevar acabo las funciones de gestión requeridas por la "Estación Gestora" actuando como servidores suministrando la información al gestor.
- Protocolo de Gestión de Red: Define la comunicación entre los nodos gestionados y las estaciones gestoras. El protocolo depende del modelo de gestión utilizado.

3 Gestión de Redes- Antonio Martín Montes, Carlos León de Mora – 2002, Página 3

- MIB (Management Information Base), es el conjunto de información del objeto gestionado, se encuentra ubicado en el dispositivo de telecomunicación.

1.1.3 Arquitectura de Gestión de Red

En el esquema de funcionamiento de una plataforma de gestión, el usuario a través de una interfaz unificada tiene acceso a la información procedente de las diversas aplicaciones de gestión (gestores). Esto se requiere así, puesto que la diversidad de elementos de red procedentes de diferentes fabricantes junto con la enorme cantidad de funciones de gestión definidas por los estándares, aconseja el procesado en paralelo.[4]

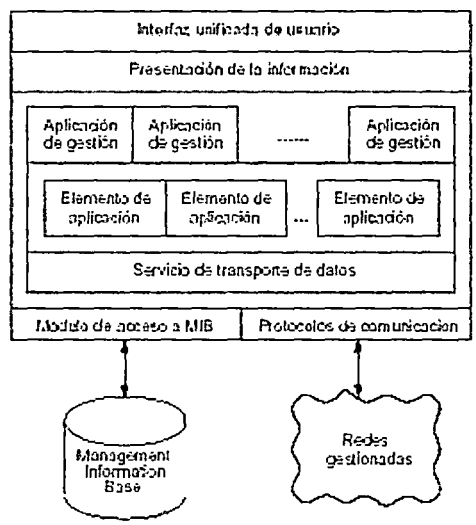


Ilustración 2 Esquema de Funcionamiento de una plataforma de gestión[5]

Dado que los sistemas distribuidos y las redes de área local tienen un carácter abierto, es necesario definir arquitecturas de gestión de red normalizadas que permitan la gestión de elementos heterogéneos de múltiples proveedores. Siendo los estándares más extendidos los siguientes:

- Modelo de Gestión OSI: Arquitectura definida por ISO, utiliza CMIS/CMIP (Common Management Information Service/ Common Management Information Protocols). Constituye un estándar concebido para operar sobre

4 Gestión de Redes- Antonio Martín Montes, Carlos León de Mora – 2002, Página 5

5 Gestión de Redes- Antonio Martín Montes, Carlos León de Mora – 2002, Página 6

protocolos OSI. Si bien puede operar, a nivel de aplicación sobre otros protocolos, sea el caso de TCP/IP, para cuyo caso se denomina CMOT (Common Management Over TCP/IP).

- Modelo de Gestión Internet: Utiliza SNMP(Simple Network Management Protocol), estándar de facto que opera sobre el protocolo TCP/IP
- Modelo de Gestión TMN: Definida por la ITU-T, se basa en los modelos anteriores e incluye el acceso a los recursos de telecomunicaciones.

Y puesto que el modelo de Internet es el que más se asemeja a las características de nuestra red, más adelante, se tendrá más detalle sobre este

1.2 Monitoreo de Redes.

1.2.1 Introducción:

Todo sistema creado sea pequeño o grande siempre estará expuesto a amenazas, conflictos y caídas. Y es por esto la gran importancia de un sistema de monitoreo, para tratar de tener siempre un escenario claro del estado de nuestra red.

Y es así que se define por Monitoreo de la red a las acciones consistente en obtener información de la red con el fin de detectar anomalías, estas acciones son pasivas y su único objetivo es conocer el comportamiento de los recursos monitorizados.[6]

Los objetivos de la monitorización son principalmente la prevención de incidencias y conocer el aprovechamiento de los recursos TIC disponibles. Dado que estos objetivos son importantes en cualquier entidad independientemente de su tamaño, es evidente que toda organización debería contar con su propio sistema de monitorización.

1.2.2 Definición de la información a monitorizar: La información se puede clasificar en:

- Estática: Caracteriza la configuración de los recursos y cambia con muy poca frecuencia.

6 Gestión de Redes- Antonio Martín Montes, Carlos León de Mora – 2002, Página 4

- Dinámica: Asociada a eventos que se da en la red. Dentro de este segundo tipo vamos a tener la información estadística, obtenida al procesar la información dinámica.

1.2.3 Forma de acceso a la información de monitorización: Por parte de los módulos gestores a los módulos agentes que se localizan en los recursos, el acceso se realiza mediante los denominados protocolos de intercambio de información de gestión, punto clave en el monitoreo de red.

1.2.4 Diseño de mecanismos de monitorización: Se fundamenta en un sondeo periódico por parte del gestor a los agentes, preguntando por los dato de monitorización. Existe además el mecanismo de informe de eventos, en el cual los agentes informan por propia iniciativa a los gestores ante un cambio de estado significativo.

1.2.5 Procesado de la información de monitorización obtenida: Dándole un tratamiento que dependerá de la función para la que se ha realizado la monitorización.

1.3 Modelo de Gestión Internet:

Sistema de gestión basado en el protocolo SNMP (Simple Network Management Protocol), el marco de trabajo de este protocolo se rige principalmente a los siguientes documentos:

- Structure of Management Information (SMI): RFC1155, Describe como se definen en la MIB los objetos gestionados.
- Management Information Base (MIB): RFC 1156, RFC 1213, Define los objetos almacenados en la MIB.
- Simple Network Management Protocol (SNMP): RFC 1157, describe el protocolo para gestionar los objeto[7]

1.3.1 Estructura de la Información de Gestión (SMI, Structure of Management Information): El objetivo de especificar una estructura de la información de gestión consiste en poder referenciar un recurso en un sistema remoto. Pero para ello se requieren una serie de elementos, como un protocolo IP que nos permite llegar al sistema remoto, o el protocolo SNMP que permite llegar al proceso de gestión de red del sistema remoto. Sin embargo, existe un problema: ¿Cómo llegar a los

7 Modelo de Gestión de Red, Grupo SSI Página 5

recursos del sistema remoto?, para ello se va a utilizar un método común para nombrar a los objetos. Este método usa los identificadores de objetos (Object Identifiers, OID).[8]

1.3.1.1 Identificadores de Objetos (OID, Object Identifiers): Los OID no son más que una secuencia de enteros no negativos separados por un punto que forman un árbol. Este árbol, denominado de registro, está estandarizado a nivel mundial. Por ejemplo, el OID 1.3.6.1.1 identifica el objeto que se encontraría si, comenzando en el root, pasamos a la rama 3, después a la 6, a la 1 y finalmente a la rama 1.

El árbol está formado por ramas y nodos. En cada nodo existe una etiqueta consistente en un número entero y quizás un texto breve. Cada nodo puede tener nodos hijos (subordinados o sub-identifiers), conectados a éste mediante líneas (ramas). El árbol comienza con un nodo inicial denominado root que se puede extender hasta cualquier nivel de profundidad.

Estos OIDs son los que permiten alcanzar (nombrar) objetos mediante SNMP. Pero ¿Cómo devolvemos los valores de los objetos (respuesta a un get)?. Para que ello sea posible es necesario conocer la estructura de los valores que nos pueden llegar desde los objetos, es decir la Macro OBJECT-TYPE, así como conocer el uso de una codificación por línea conocida de estos valores, esto se define utilizando Abstract Syntax Notation One (ASN.1)

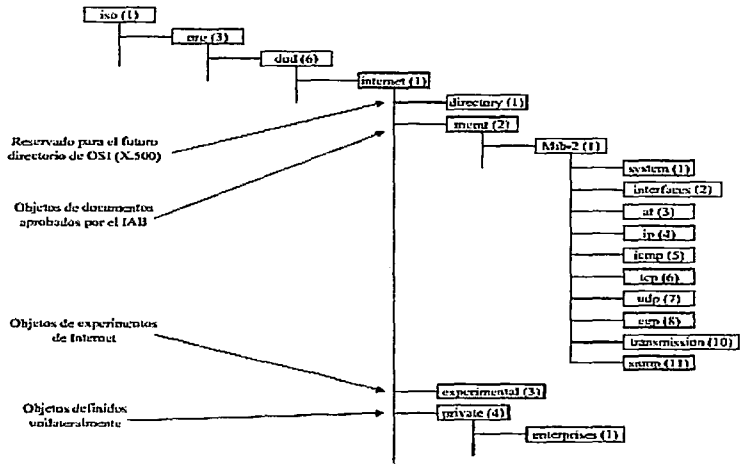


Ilustración 3 Árbol de Registro9

8 Gestión de Red- Antoni Barba Martí- Edición UCP 1999, Página 156

9 Modelo de Gestión de Red, Grupo SSI, Página 8

1.3.1.2 Sintaxis ASN.1 (Abstract Syntax Notation One): La sintaxis ASN.1, que se representa mediante el término Syntax en la macro de tipo de objetos, define el tipo de datos que modela el objeto. La sintaxis abstracta se utiliza para describir tanto las estructuras de datos que se intercambian las entidades del protocolo SNMP como la información de gestión que contienen estas estructuras de datos.

Junto con el concepto de sintaxis abstracta, existe el concepto de sintaxis de transferencia. Ésta última permita a partir de la definición de las estructuras de datos, utilizar una forma determinada de transmitir los datos a través de la red. La sintaxis de transferencia que se utiliza junto con la ASN.1 son las reglas de codificación básicas (BER)

Si bien se usa ASN.1 para la sintaxis abstracta, dado que esta notación es muy extensa, se restringe su uso para mantener la simplicidad en los agentes.[10]

Se definen tres tipos de objetos con ASN.1:

- Tipos (types): Que definen nuevas estructuras de datos.
- Valores (values), Son realizaciones (variables) de un tipo.
- Macros: Se utilizan para cambiar la gramática ASN.1.

Para saber en cada momento de que tipo de object se trata, se utiliza la siguiente regla. Los identificadores de tipo comienzan en mayúscula, los identificadores de valor se escriben en minúscula y los identificadores de macros se escriben completamente en mayúsculas.

Así por ejemplo el tipo se representa con la siguiente sintaxis:

NombreDeTipo = TIPO

Existen una serie de tipos permitidos para los objetos que se utilizan en el protocolo de gestión:

- Tipos Simples: Entre los cuales tenemos:

  ✓ Integer: Toma como valor un número entero.

10 Gestión de Red- Antoni Barba Martí- Edición UCP 1999, Página 157.

- ✓ Octet String: Toma como valor 0 o más octetos, cada byte puede tomar valores entre 0 y 255.
- ✓ Object Identifier: Tipo de dato que permite la identificación de objetos de gestión.

- Tipos Estructurados: Entre los cuales tenemos:
  - ✓ Sequence: Tipo de dato para hacer listas
  - ✓ Sequence Of: Tipo de dato para hacer tablas

Junto a estos tipos, es preciso definir también en las macros de los objetos gestionados un acceso y un estatus para así poder especificar las operaciones permitidas en éstos. El acceso (Access) define el nivel de acceso al objeto y puede especificarse uno de los siguientes:

- Solo lectura (Read – Only)
- Lectura y Escritura (Read – Write)
- Solo lectura (Write – Only)
- No accesible (Not – Accesible)

El status permite definir los requisitos de implementación del objeto distinguiéndose los siguientes:

- Mandatorio (Mandatory, el único que se utiliza actualmente)
- Opcional (Optional)
- Obsoleto (Obsolete).

Por otra parte, el nombre de los objetos se define como un OBJECT IDENTIFIER que se usa para nombras a los objetos gestionados. Este identificador puede estar en tres tipos de MIBs. Estas son actualmente las siguientes:

- MIB estándar de Internet: mib OBJECT IDENTIFIER
- MIB Experimental: experimental OBJECT IDENTIFIER
- MIB privadas: enterprises OBJECT IDENTIFIER

1.3.2 Bases de Información de Gestión (MIB, Management Information Base): Las MIB son un conjunto de objetos gestionados de un recurso que se publica para ofrecer la interoperabilidad de gestión. Actualmente existen los siguientes tipos de MIBs, las estándares que son la MIB-I y MIB - II; las experimentales, con grupos en fase de desarrollo y, finalmente, las privadas, que incorporan la información de los diversos fabricantes de equipos.

1.3.2.1 MIB-I: Constituye la primera MIB normalizada. Está formada con objetos de la torre de protocolos de TCP/IP. En la figura se especifican los grupos que la forman, con el número de objetos que forman cada grupo y una breve descripción de éstos.[11]

Grupo	Número	Propósito
system	3	El propio sistema
interfaces	22	Interfaces de red
at (adress translation)	3	Correspondencia de dirección IP
ip	33	Protocolo internet
icmp	26	P. de mensaje de control internet
tcp	17	P. de control de transmisión
udp	4	P. de datagrama de usuario
egp	6	P. de pasarela exterior
	114	

Ilustración 4 Esquema de grupos de la MIB - I[12]

1.3.2.2 MIB-II: Se realizaron una serie de modificaciones sobre la primera versión. Entre éstas se halla la de la tabla "address translation" que se desestimó. También se define un nuevo grupo para cada tipo específico de interfaz, así como un nuevo grupo con objetos de SNMP.

11 Gestión de Red- Antoni Barba Martí- Edición UCP 1999, Página 164.

12 Gestión de Red- Antoni Barba Martí- Edición UCP 1999, Página 164.

Grupo	Número	Comentarios
system	7	eran 3
interfaces	23	eran 22
at	3	serán 0
ip	38	eran 33
icmp	26	sin cambio
tcp	19	eran 17
udp	7	nueva tabla
egp	18	expansión de tabla
transmission	0	nuevo
snmp	30	nuevo
	171	

Ilustración 5 Esquema de grupos de la MIB - I13

1.3.2.3 MIBs Experimentales: Las MIB experimentales son las MIB consideradas en fase de desarrollo por los grupos de trabajo de Internet. Actualmente existen MIBS para: IEEE 802.4 Token Bus, IEEE 802.5 Token Ring, RMON, entre otros.14

1.3.2.4 MIBs Privadas: Las MIB privadas corresponden a las MIBs de productos específicos, generadas por los distintos fabricantes y añaden funcionalidades a las MIB estándar. Generalmente, los fabricantes las hacen públicas, poniéndolas accesibles por Internet.15

1.3.2.5 Los Objetos: Se accede a los objetos gestionados a través de una tienda virtual de información denominada la base de información de gestión (MIB).

Los Objetos en la MIB se definen usando ASN.1. En particular, cada objeto tiene un nombre, una sintaxis y una codificación. El nombre es un identificador del objeto, un nombre asignado administrativamente, que especifica el tipo de objeto. El Tipo de objetos junto con la instancia del objeto sirve para identificar de forma única una específica instanciación del objeto. Por conveniencia humana, A menudo se utiliza una cadena de texto, denominada DESCRIPCIÓN DEL OBJETO, que también hace referencia al tipo de objeto.

La sintaxis de un tipo de objeto define la estructura de datos abstracta correspondiente a ese tipo de objeto. El lenguaje ASN.1 se utiliza para este

13 Gestión de Red- Antoni Barba Martí- Edición UCP 1999, Página 164.

14 Gestión de Red- Antoni Barba Martí- Edición UCP 1999, Página 168.

15 Gestión de Red- Antoni Barba Martí- Edición UCP 1999, Página 169

propósito. Sin embargo, a propósito se restringen las construcciones ASN.1 que se pueden utilizar. Estas restricciones son hechas explícitamente para mantener la simplicidad.

La codificación de un tipo de objeto es simplemente cómo se representa ese tipo de objeto utilizando su sintaxis. Implícitamente vinculada a la noción de la sintaxis de un tipo de objeto y la codificación es cómo se representa el tipo de objeto que se va a transmitir en la red. Esta nota especifica el uso de las reglas básicas de codificación de ASN.1

Grupos de objetos: Esta lista de objetos gestionados contiene sólo los elementos esenciales, no hay necesidad de permitir que los objetos individuales sean una opción. Más bien, los objetos se disponen en los siguientes grupos: [16]

- Sistema
- Interfaces
- Traducción de direcciones
- IP
- ICMP
- TCP
- UDP
- EGP
- Transmisión
- SNMP

Hay dos razones para la definición de estos grupos: uno, para proporcionar un medio de asignación de identificadores de objetos; dos, para proporcionar un método para implementaciones en los agentes, para que estos sepan qué objetos deben implementar. Este método es el siguiente: si la semántica de un grupo es aplicable a una aplicación, entonces se debe poner en práctica todos los objetos en ese grupo. Por ejemplo, se debe implementar el grupo EGP si y sólo si se implementa el protocolo EGP.

16 RFC1156 Management Information Base (MIB)

- Formato: La siguiente sección contiene la especificación de todos los tipos de objetos contenidos en el MIB. Los tipos de objetos se definen mediante los siguientes campos:

- OBJETO: Un nombre textual, denominado DESRIPCIÓN DEL OBJETO, para el tipo de objeto, junto con su correspondiente identificador de objeto.

- Sintaxis: La sintaxis abstracta para el tipo de objeto, para la cual se utiliza ASN.1. Esto se debe resolver en una instancia del ObjectSyntax tipo ASN.1 definida en el SMI.

- Definición: Una descripción textual de la semántica del tipo de objeto. Las implementaciones deben asegurarse de que su interpretación del tipo de objeto cumple con esta definición ya que este MIB es para uso en entornos de proveedores múltiples. Como tal, es vital que los tipos de objetos tengan un significado consistente a través de todas las máquinas.

- Acceso: Una de sólo lectura, lectura y escritura, de sólo escritura, o no accesible.

- Estado: Uno de obligatorios, opcionales u obsoleta.[17]

1.3.3 Simple Network Management Protocol (SNMP): El protocolo SNMP surge a partir del protocolo SGMP para gestión de routers IP. SNMP es un protocolo de aplicación que ofrece servicios de gestión de red al conjunto de protocolos de Internet. SNMP define una arquitectura basada en cliente – servidor.[18]

1.3.3.1 Arquitectura de SNMP: La arquitectura SNMP es una colección de estaciones de administración de red y elementos de red.

Las estaciones de administración de red ejecutan aplicaciones de gestión que supervisan y Controlan a los elementos de la red.

Los elementos de red son dispositivos tales como ordenadores, gateways, servidores de terminales, y similares, que tienen agentes de gestión encargados de desempeñar las funciones de gestión de red solicitada por las estaciones de administración de red. [19]

17 RFC1156 Management Information Base (MIB)

18 Gestión de Red- Antoni Barba Martí- Edición UCP 1999, Página 169

19 RFC1157 Simple Network Management Protocol (SNMP)

Los agentes de gestión mantendrán una MIB local, atenderán solicitudes de la estación de gestión y podrán enviar de manera asíncrona informes de eventos importantes (event reporting). Soporta por tanto los dos mecanismos de comunicación agente-gestor que conocemos.

La MIB local de cada agente mantiene información sobre objetos del recurso que gestiona almacenada en forma de pares atributo-valor. Los objetos están estandarizados para recursos del mismo tipo (todos los concentradores tendrán los mismos objetos).

El Simple Network Management Protocolo (SNMP) se utiliza para comunicar la información gestionada entre las estaciones de administración de red y los agentes en los elementos de red. El protocolo es muy simple, proporcionando las siguientes posibilidades:

- Get: permite a la estación gestora obtener valores de objetos de agentes.
- Set: permite a la estación gestora modificar valores de objetos de agentes.
- Trap: permite a un agente enviar de manera asíncrona la notificación de un evento importante a la estación de gestión.[20]

En el estándar no se indica nada acerca del número de estaciones gestoras o del ratio gestores/agentes, aunque lo normal es tener dos estaciones gestoras (una de backup) y al ser el protocolo simple, el número de agentes por gestor puede ser bastante alto (centenares).

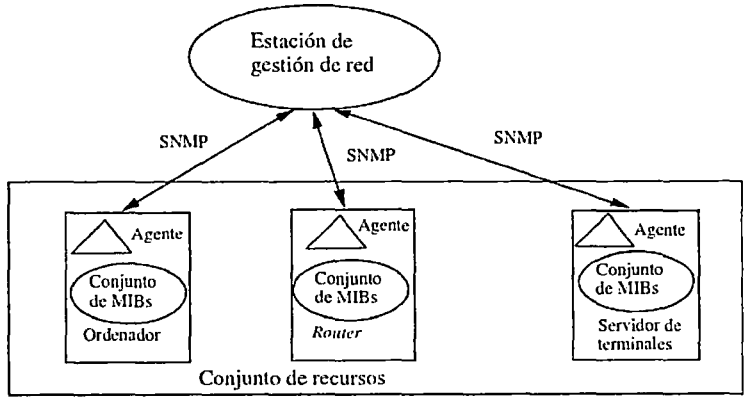


Ilustración 6 Arquitectura de un Sistema de Gestión SNMP[21]

20 Modelo de Gestión de Red, Grupo SSI, Página 11.

1.3.3.2 Objetivos del Protocolo SNMP: El principal objetivo del SNMP es minimizar explícitamente el número y la complejidad de las funciones realizadas por el agente de gestión. Este objetivo es atractivo en al menos cuatro aspectos:

- El costo de desarrollo para el software del agente de gestión necesario para apoyar el protocolo se reduce en consecuencia.
- El grado de la función de gestión que es soportado remotamente en consecuencia se incrementa, admitiendo con ello plena utilización de los recursos de Internet en la tarea de gestión.
- El grado de la función de gestión que es soportado remotamente en consecuencia se incrementa, imponiendo así la menor cantidad de restricciones posibles sobre la forma y sofisticación de las herramientas de gestión.
- Simplifica el conjunto de las funciones de gestión haciéndolas fácilmente comprendidas y utilizadas por los desarrolladores de herramientas de gestión de red.

Un segundo objetivo del protocolo es que el paradigma funcional para vigilancia y control sean lo suficientemente extensible para incluir aspectos adicionales, posiblemente no previstos en la operación y gestión de la red.

Un tercer objetivo es que la arquitectura sea, tanto como sea posible, independiente de las arquitecturas y mecanismos de hosts o puertas de enlaces particulares.[22]

1.3.3.3 Envió y Recepción de un Mensaje SNMP:

- Secuencia de transmisión de un mensaje SNMP
  - ✓ Construcción de la PDU, usando estructuras ASN.1.
  - ✓ La PDU se procesa por el servicio de autenticación junto a las direcciones correspondientes.
  - ✓ La entidad de protocolo construye el mensaje, consistiendo de una versión de campo, el nombre de la comunidad y el resultado del paso anterior.

---

21 Gestión de Red- Antoni Barba Martí- Edición UCP 1999, Página 169

22 RFC1157 Simple Network Management Protocol (SNMP)

- ✓ Este nuevo objeto ASN.1 es entonces codificado, usando las reglas de codificación básicas y pasado al servicio de transporte.

  En la práctica, las autentificaciones no se invocan.

- Secuencia de Recepción de un mensaje SNMP.

  - ✓ Chequeo básico de la sintaxis del mensaje, descartándolo si es erróneo.
  - ✓ Verificación del número de versión. Se descarta el mensaje si no es coherente.
  - ✓ La entidad de protocolo pasa al usuario la porción PDU del mensaje y las direcciones de transporte de emisor y receptor al servicio de autenticación.
  - ✓ Si la autenticación falla, el servicio de autenticación señaliza a la entidad de protocolos SNMP, para que genere una Trap y descarte el mensaje.
  - ✓ Si la autenticación tiene éxito, el servicio de autenticación devuelve la PDU en la forma de objeto ASN.1 definido en RFC1157.
  - ✓ La entidad de protocolo hace un chequeo básico de la sintaxis del mensaje, descartándolo si es erróneo. En cualquier caso, la comunidad nombrada con la adecuada política de acceso SNMP seleccionada finalmente procesa la PDU.

1.3.3.4 Marco administrativo: Para una gestión adecuada con SNMP se define un nombre de comunidad (community) que afecta tanto al agente como al conjunto de gestores que lo administran, y un perfil de comunidad que delimita las propiedades así como el modo de acceso al sistema. De esta forma, la comunidad puede ser pública (public), es decir, de libre acceso. Esta información se almacena en cada MIB. De esta forma, una comunidad es una relación entre un agente y gestores y el nombre de comunidad es una cadena de octetos transmitida en los mensajes SNMP.

Para la determinación de políticas de autentificación y autorización se trabaja con autentificación simple, en la que el nombre de comunidad se transmite en claro; de ahí la necesidad de ampliar la seguridad del entorno de gestión mediante otros servicios de seguridad. En cuanto a la autorización cada comunidad tiene asociado una vista (conjunto de objetos), de forma que para cada objeto se define un modo de acceso:

read-only, read-write. Finalmente, el nombre de comunidad junto al perfil de comunidad marca la política de acceso al sistema.[23]

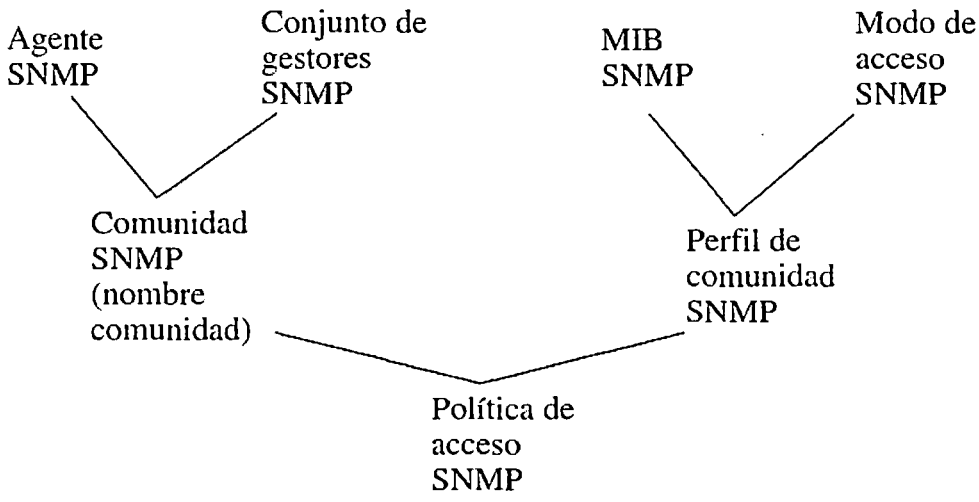


Ilustración 7 Conceptos Administrativos[24]

1.3.4 SNMPv2: Este protocolo de gestión que se definió en 1993, es una versión más avanzada del protocolo SNMP. SNMPv2 aporta una serie de ventajas respecto a la primera versión, entre las cuales pueden destacarse:

- Permite una mayor eficiencia en la transferencia de información.
- Admite mecanismos de seguridad como la autentificación y el cifrado frente al SNMP (no implementados).
- Permite la comunicación entre estaciones de gestión.
- Parte de un modelo de comunicaciones extendido considerablemente.
- Permite una señalización extendida de errores.
- Permite el uso de varios servicios de transporte.

23 Gestión de Red- Antoni Barba Martí- Edición UCP 1999, Página 175

24 Gestión de Red- Antoni Barba Martí- Edición UCP 1999, Página 175

El sistema basado en SNMPv2 soluciona muchos de los problemas de su anterior versión, SNMP; sin embargo, su mayor complejidad está coartando su desarrollo.

Los mensajes enviados por la plataforma de gestión de red a los agentes SNMP están formados por identificadores de objetos MIB junto con instrucciones, a fin de cambiar u obtener un valor.[25]

1.3.4.1 Operaciones de SNMPv2: El protocolo SNMPv2, que incluye los mensajes de la primera versión SNMP, dispone de los siguientes tipos de mensajes:

- Get Request: Petición de valores específicos de la MIB.
- Get Next Request: proporciona un medio para moverse por la MIB. Petición del objeto siguiente a uno dado de la MIB.
- Get Bulk Request: Petición de múltiples valores.
- Response: devuelve los valores solicitados por las operaciones anteriores gestor a gestor o agente a gestor.
- Set Request: Permite asignar un valor a una variable. Debido a posibles problemas de seguridad esta función suele estar desactivada.
- Inform Request: transmite información no solicitada (gestor a gestor).
- SNMPv2 - Traps: Permite a los agentes informar de sucesos inusuales.

Sin embargo, el hecho de su incompatibilidad con la versión SNMP y la mayor complejidad añadida a las plataformas están desestimando su futura implementación.

El desacuerdo en el consorcio sobre las recomendaciones acerca de seguridad propuestas en SNMPv2 ha propiciado finalmente su incorporación en una nueva versión SNMPv3.[26]

1.3.5 SNMPv3: El protocolo SNMPv3 es una evolución de la serie de modelos de gestión vistos anteriormente. SNMPv3 está aún en fase de especificación; sin embargo, se pueden describir algunas de las características en las que se está trabajando. Las

25 Gestión de Red- Antoni Barba Martí- Edición UCP 1999, Página 178

26 Gestión de Red- Antoni Barba Martí- Edición UCP 1999, Página 179

áreas a las que SNMPv3 va enfocado son, primordialmente, mejorar la seguridad y la administración respecto a SNMPv2.

Respecto a la estructura de la información de gestión, la SMI está dividida en tres partes: definiciones de módulos, definiciones de objetos y definiciones de notificaciones. Las definiciones de módulos se utilizan para describir semánticamente los módulos de información. Para las definiciones sintácticas y semánticas de objetos se usan macros ASN.1:

OBJECT - TYPE. Las definiciones de notificaciones usan macros NOTIFICATION-TYPE y describen transmisiones no solicitadas de información de gestión.

Entre los tipos de datos que se incorporan a la SMI (RFC1902) están:

- IMPORTS para permitir la especificación de items que se usan en un módulo MIB, pero definidos en otro módulo MIB
- MODULE-IDENTITY especifica una descripción e información administrativa para un módulo MIB.
- OBJECT-IDENTITY y los OID se asignan para especificar un valor OID.
- OBJECT-TYPE especifica el tipo de dato, estatus y la semántica de los objetos gestionados.
- SEQUENCE es un tipo que permite asignar los objetos de una lista en una tabla.
- NOTIFICATION-TYPE se especifica para construir una notificación de eventos.

En SNMPv3 se prevé también aumentar el mapeo de mensajes tipo SNMP a otros tipos de protocolos de transporte. Desde el punto de vista de arquitectura de gestión se extiende el nombrado de:

- Motores y aplicaciones
- Entidades
- Identidades
- Información de gestión, incluido soporte para múltiples contextos lógicos

Los cinco tipos de aplicaciones que se prevé asociar con un motor SNMP son: generadores de comandos, receptores de comandos (generadores de

respuestas), originadores de notificaciones, receptores de notificaciones y envío de proxies.

Respecto a las mejoras en seguridad, SNMPv3 utilizará MD5 y algoritmos de Hash para firma digital, y proteger contra la modificación de la información proporcionando integridad de datos, autentificación de origen y usuario.[27]

27 Gestión de Red- Antoni Barba Martí- Edición UCP 1999, Página 181

CAPÍTULO II

RED PRIVADA VIRTUAL (VPN)

CAPÍTULO II

RED PRIVADA VIRTUAL (VPN)

2.1 Introducción:

Las redes virtuales encuentran su máxima expresión cuando nos encontramos en la siguiente situación: Un usuario autentificado en una LAN, esencialmente corporativa, precisa conectarse a ésta y a sus medios y recursos compartidos desde un punto o enlace exterior. Este es el caso típico de un usuario conectado a la LAN de su empresa vía Internet. Como respuesta a esta necesidad, se ha implementado lo que ha venido a denominarse Redes Privadas Virtuales o en inglés, Virtual Private Network (VPN).

Ángel Cobo la define como una extensión de una red privada que utiliza enlaces como Internet y que posibilita la transmisión de datos como si de un enlace punto a punto se tratase.[28]

Este tipo de redes facilitan que las compañías vean reducidos sus costes de conexión sin sufrir mermas en la seguridad de las comunicaciones. Puesto que una VPN sirve para transmitir datos de manera segura por una red que, de por sí, es de naturaleza no segura. En estos tiempos de Internet, significa que las compañías que antes alquilaban líneas de datos para conseguir seguridad en sus transacciones, ahora puedan utilizar internet para sus comunicaciones privadas. Significa también que los usuarios corporativos que estén de viaje, o en sus domicilios, pueden conectarse con un proveedor de servicios de Internet (ISP) y comunicarse de manera segura con la red corporativa, por medio de internet, sin necesidad de conectarse mediante una línea específica con la red corporativa.[29]

2.2 Funcionamiento de una VPN

Para implementar una VPN, los datos son encapsulados utilizando un protocolo de túnel, que consiste en añadir al paquete original (que usualmente pertenece al

---

28 Estudio Científico de las redes de Ordenadores - Angel Cobo Yera - Edición Visión Libros 2009, Página 178

29 Fundamentos de Telemática - Jorge Lázaro Laporta, Marcel Miralles Aguiñiga - Edición UPV 205 , Página 223

conjunto de protocolos TCP/IP) una cabecera que proporciona la información de encaminamiento, lo que le permite atravesar la red para llegar a su destino.

Para que el enlace sea privado, es decir opaco a terceros, todos los datos que lo atraviesan son cifrados, con lo que se garantiza su confidencialidad, ya que los paquetes pueden ser interceptados en la red exterior, pero son difícilmente descifrables si no se poseen las claves de cifrado.

De este modo, un enlace sobre un medio compartido en el cual los datos son encapsulados y cifrados se conoce como una conexión de red privada virtual, y es así que la principal función de una red privada virtual es permitir que los datos internos de una organización viajen de manera segura a través de una red pública no confiable como por ejemplo internet.[30]

Imaginemos un usuario A que se encuentra en el interior de una filial situada en Chiclayo, que desea conectarse a un servidor D situado en la sede principal de la empresa en Lima. Para ello, deberá comunicarse a través de Internet pero, anteriormente, atravesará el servidor VPN (B) que cifrará los datos. A la llegada, el servidor VPN (C) descifrará los datos que transmitirá sin cifrar al servidor D.

La operación es transparente, tanto para el usuario A como para el servidor D. No es necesaria ninguna otra configuración en ninguna de las dos máquinas.

La VPN permite cifrar de manera global todas las comunicaciones que circulan entre el usuario y el servidor, independientemente del protocolo utilizado (Web, mail, ftp, etc.).

Así, implementando una VPN en el interior de una empresa, se tiene la posibilidad, en una sola operación de asegurar la confidencialidad de todas las comunicaciones que circulan entre los dos sitios.

30 Estudio Científico de las redes de Ordenadores - Angel Cobo Yera - Edición Visión Libros 2009, Página 178

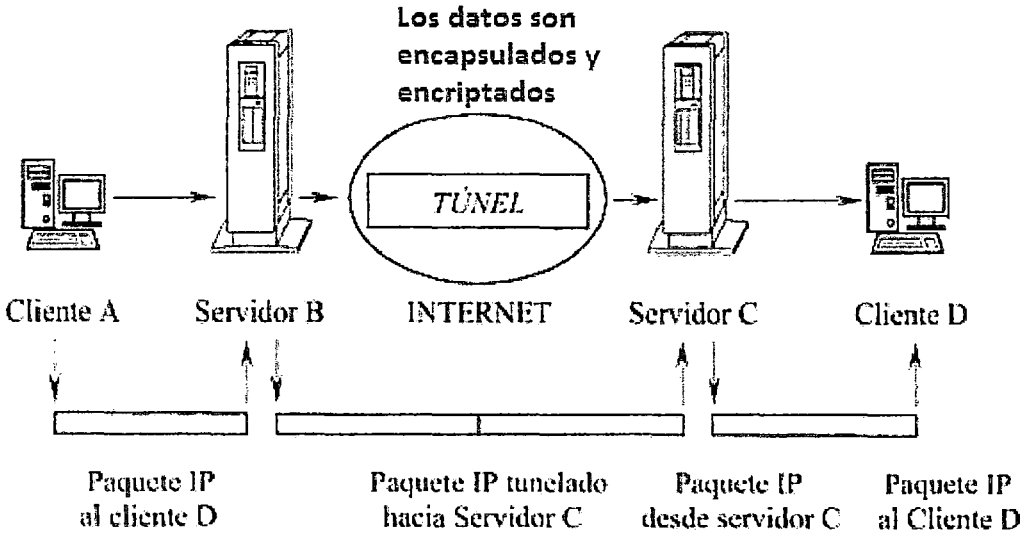


Ilustración 8 Establecimiento del Túnel en una VPN[31]

La configuración de una red privada virtual se basa principalmente en la tecnología que se implementa para el cifrado de la información. Las características globales de las principales tecnologías de VPN se muestran en la siguiente imagen:

31 Fundamentos de Telemática - Jorge Lázaro Laporta, Marcel Miralles Aguiñiga - Edición UPV 205 , Página 224

Tecnología	*Puntos fuertes*	*Puntos débiles*	*En desarrollo*
IPSEC	• Opera independiente de las aplicaciones de niveles superiores • Subconjunto de IPv6 • Ocultación de direcciones de red sin emplear NAT • Acoplamiento con las técnicas criptográficas existentes y futuras	• No proporciona la gestión de usuarios • Interoperabilidad entre los fabricantes. • No estandarizado	• Estandarización de todas las facetas de PKI, incluyendo los protocolos de intercambio de certificados y el formato de éstos. • El IETF está en su desarrollo
Cortafuegos	• Gestión centralizada de los parámetros de seguridad, autenticación y acceso. • Disponibilidad de una interfaz común para la modificación de las reglas del túnel. • Disponibilidad de ACLs para usuarios remotos.	• Reducción del modo de operación debida a la encriptación software. • Precisa un alto control con los cambios al añadir nuevas reglas VPN.	• Mismos objetivos que IPSec. • Soluciones capaces de realizar la encriptación por medio del hardware
PPTP	• Soporta tunneling extremo a extremo y entre servidores. • Posibilidad de valor añadido para el acceso remoto. • Proporciona una capacidad multiprotocolo. • Empleo de encriptación RSA RC-4	• No proporciona encriptación de datos para los servidores de acceso remoto • Precisa un servidor NT como terminador del túnel. • Sólo usa encriptación RSA RC-4	• Integración con IPSec
L2F	• Habilita el tunneling multiprotocolo • Soportado por la gran mayoría de fabricantes	• No posee encriptación • Autenticación débil • No dispone de control de flujo sobre el túnel	• Implementaciones que empleen el nombre de usuario y dominio en el establecimiento del túnel
L2TP	• Combina L2F y PPTP. Necesidad de únicamente una red de paquetes para operar bajo X.25 y Frame Relay.	• Aún no implementado	• Estandarización y operación en proceso • Será adoptado por los fabricantes para el acceso remoto una vez completo
VTCP/Secure	• Mecanismos de encriptación y autenticación fuerte. • Proporciona seguridad extremo a extremo. • Tunneling basado en nombre de dominio.	• Protocolo propietario. • Las configuraciones LAN-LAN no están permitidas. • No es multiprotocolo.	• Compatibilidad con IPSec.

Ilustración 9 Comparativa global entre las diferentes tecnologías VPN[32]

32 Herramientas para circuitos y redes virtuales: interconectividad global segura- Sergio Gonzalo San José, Página 7

Se decidió utilizar la tecnología PPTP para la creación de las VPNs por ello a continuación se describirá con más detalle el protocolo PPTP.

2.3 **El Protocolo de Túnel Punto a Punto (PPTP, Point-to-Point Tunneling Protocol)**: Es una extensión del protocolo punto a punto PPP, el cual es utilizado tradicionalmente para las conexiones dial-up. El protocolo PPTP fue desarrollado en modo propietario por Microsoft, Ascend Communications y US Robotics, este permite la realización de transferencias seguras desde clientes remotos a servidores emplazados en redes privadas, empleando para ello tanto líneas telefónicas conmutadas como Internet.

PPTP opera en la capa 2 del modelo OSI y utiliza el puerto 1723 y el Id. 47, en su escenario típico, el cliente establecerá una conexión dial-up con el servidor de acceso a red (NAS) del proveedor del servicio, empleando para ello el protocolo PPP. Una vez conectado el cliente establecerá una segunda conexión con el servidor PPTP el cual estará situado en la red privada. Dicho servidor será utilizado como intermediario de la conexión, recibiendo los datos del cliente externo y transmitiéndolos al correspondiente destino en la red privada. [33]

PPTP fue normalizado por el IETF en el RFC 2637, el cual nos dice que este protocolo de red permite encapsular las tramas del protocolo punto a punto PPP en datagramas IP para su transmisión a través de una red IP. PPTP no especifica ningún cambio en el protocolo PPP sino que describe un nuevo vehículo para la realización de PPP. Una arquitectura cliente-servidor se define con el fin de desacoplar las funciones que existen en los servidores de acceso de red actuales (NAS) y apoyar a las redes privadas virtuales (VPN). PPTP utiliza un mecanismo extendido de GRE (Generic Routing Encapsulation) para encapsular en un datagrama los paquetes PPP. [34]

2.3.1 Estructura de PPTP

2.3.1.1 Concentrador de Acceso PPTP (PAC): El Concentrador de Acceso PPTP (PAC, PPTP Access Concentrator) es un dispositivo conectado a las líneas PSTN o ISDN capaz de realizar operaciones PPP y de manejar el protocolo PPTP. Lo único que necesita el PAC es implementar TCP/IP para transportar el tráfico hacia uno o más PNS. También puede

33 Herramientas para circuitos y redes virtuales:interconectividad global segura- Sergio Gonzalo San José, Página 5

34 RFC 2637 Point-to-Point Tunneling Protocol (PPTP)

entunelar protocolos que no son IP. Es también conocido como FEP o Procesador Final Frontal.

2.3.1.2 Servidor de Red PPTP (PNS): El Servidor de Red PPTP (PNS, PPTP Network Server) es un dispositivo que opera como un servidor de túnel. Puesto que PPTP se basa completamente en TCP/IP y es independiente de la interface de hardware, el PNS puede utilizar cualquier combinación de hardware incluyendo dispositivos LAN y WAN.

2.3.2 División de las Funciones Del NAS: PPTP permite a las funciones existentes del Network Access Server (NAS) separarse utilizando una arquitectura cliente-servidor. Tradicionalmente, las siguientes funciones son ejecutadas por un NAS:

a. La interconexión física natural a un PSTN o RDSI y el control de los módems externos o adaptadores de terminal. Un NAS puede conectarse directamente a un circuito análogo o digital de la compañía de telecomunicaciones o conectarse a través de un módem externo o adaptador de terminal. El control de una conexión de conmutación de circuitos se lleva a cabo, ya sea con el control de módem o con protocolos de control de llamada RDSI DSS1. El NAS, en conjunción con el módem o adaptadores de terminal, puede realizar la adaptación de velocidad, conversión de analógico a digital, conversión de síncrona a asíncrona u otras alteraciones de los flujos de datos.

b. Terminación lógica de una sesión del protocolo punto a punto (PPP) y del protocolo de control de enlace (LCP).

c. La participación en los protocolos de autenticación PPP.

d. La agregación de canales y gestión de paquete para el protocolo PPP Multilink.

e. Terminación lógica de varios protocolos PPP de control de red de (NCP).

f. Enrutamiento multiprotocolo y puente entre las interfaces NAS.

PPTP divide estas funciones entre el PAC y PNS. El PAC es responsable de las funciones a, b, y posiblemente c. El PNS es responsable de las funciones d, e, y f, y puede ser responsable de la función c.

El protocolo utilizado para llevar unidad de datos de protocolo (PDU) de PPP entre el PAC y el PNS, así como el control y gestión de llamadas está dirigido por PPTP.

La división de las funciones de un NAS ofrece los siguientes beneficios:

Gestión de direcciones IP flexible. Los usuarios de una línea podrán mantenerse en una única dirección IP, cuando accedan en diferentes PACs, siempre que estén asociados de un PNS común. Si una red de empresa utiliza direcciones no registradas, un PNS asociado con la empresa asigna direcciones significativas a la red privada.

Soporte de protocolos no-IP para redes dial-up detrás de las redes IP. Permite Appletalk e IPX, por ejemplo, para hacer un túnel a través de un proveedor de IP-solamente. El PAC no necesita ser capaz de procesar estos protocolos.[35]

2.3.3 Objetivos del PPTP: El protocolo PPTP es implementado sólo por el PAC y el PNS. Los otros sistemas no tienen que ser conscientes del PPTP. Las redes dial-up pueden estar conectadas a un PAC sin ser conscientes del PPTP. El software del cliente PPP estándar debe seguir funcionando en enlaces PPP túnel.

PPTP también se puede utilizar para una sesión de túnel PPP a través de una red IP. En esta configuración, el túnel PPTP y la sesión PPP se ejecuta entre las dos mismas máquinas, y el que llama actúa como un PNS.

Un solo PNS puede asociarse con muchos PACs para concentrar el tráfico de un gran número de sitios geográficamente diversos.

PPTP utiliza una versión extendida del GRE para llevar paquetes PPP de los usuarios. Estas mejoras permiten un bajo nivel de congestión y control de flujo para ser proporcionada en los túneles utilizados para transportar datos de usuario entre el PAC y el PNS. Este mecanismo permite un uso eficiente del ancho de banda disponible para los túneles y evita retransmisiones innecesarias y desbordamientos de búfer. PPTP no dicta los algoritmos particulares que se utilizarán para este control de bajo nivel, pero sí define los parámetros que deben ser comunicados con el fin de permitir que este tipo de algoritmos puedan trabajar.[36]

35 RFC 2637 Point-to-Point Tunneling Protocol (PPTP)

36 RFC 2637 Point-to-Point Tunneling Protocol (PPTP)

2.3.4 Componentes de PPTP: Los componentes de PPTP son:

2.3.4.1 Conexión de Control: Antes de que PPP pueda ser entunelado entre un PAC y un PNS, se debe establecer una conexión de control entre ambos dispositivos. La conexión de control es una sesión TCP estándar sobre la cual pasa el control de la llamada PPTP y la administración de la información. El control de la sesión está asociado lógicamente pero separado de las sesiones que son entuneladas a través de un túnel PPTP. Para cada pareja PAC-PNS existe tanto un túnel como una conexión de control. La conexión de control es responsable de establecer, administrar y liberar las sesiones transportadas a través del túnel.

Mensajes de control. PPTP define un conjunto de mensajes enviados como datos TCP en la conexión de control entre un PAC y un PNS. La sesión TCP para establecer la conexión de control es establecida al iniciar una conexión TCP en el puerto 1723. El conexión de control puede ser establecido tanto por el PNS como por el PAC. Cada mensaje inicia con una cabecera de ocho octetos fija. Dicha cabecera contiene la longitud total del mensaje, el indicador del tipo de mensaje PPTP y una constante conocida como Magic Cookie.37

La Magic Cookie es siempre enviada como la constante 0x1A2B3C4D. Su propósito es permitirle al receptor asegurarse de que está sincronizado adecuadamente con el flujo de datos TCP. Los mensajes utilizados para mantener el control de las conexiones PPTP se muestran en la siguiente figura:

37 RFC 2637 Point-to-Point Tunneling Protocol (PPTP)

Código	Nombre	Descripción
1	Start-Control-Connection-Request	Inicia el establecimiento de la sesión PPTP
2	Start-Control-Connection-Reply	Es la respuesta al mensaje 1. Contiene un código resultante que indica el éxito o el fracaso del establecimiento de la sesión así como el número de la versión del protocolo
3	Stop-Control-Connection-Request	Es una petición para cerrar el conexión de control
4	Stop-Control-Connection-Reply	Es la respuesta al mensaje 3. Contiene el código resultante que indica el éxito o fracaso del cierre de la conexión
5	Echo-Request	Enviado periódicamente tanto por el cliente como por el servidor para mantener activa la conexión
6	Echo-Reply	Es la respuesta al mensaje 5 para indicar que la conexión sigue activa
7	Outgoing-Call-Request	Es una petición enviada por el cliente para crear un túnel
8	Outgoing-Call-Reply	Es la respuesta al mensaje 7, la cual contiene un identificador único para ese túnel
9	Incoming-Call-Request	Es una petición del cliente para recibir una llamada entrante por parte del servidor
10	Incoming-Call-Reply	Es la respuesta al mensaje 9. Esta indica si la llamada entrante debería ser contestada
11	Incoming-Call-Connected	Es la respuesta al mensaje 10. Provee parámetros de llamada adicionales al servidor
12	Call-Clear-Request	Es una petición para desconectar o una llamada entrante o saliente, enviada del servidor al cliente
13	Call-Disconnect-Notify	Es una respuesta al mensaje 12 para indicar que se realizará la desconexión y las razones para hacerlo
14	WAN-Error-Notify	Notifica que un error ha ocurrido en la conexión WAN, esto es, en la interfase que soporta PPP
15	Set-Link-Info	Notifica cambios en las opciones PPP

Ilustración 10 Mensajes de Control de Conexión en PPTP[38]

38 Introduction to PPTP - Point-to-Point Tunneling Protocol

Códigos de error. Los códigos de error determinan si ocurrió un error en la conexión PPTP

Código	Nombre	Descripción
0	None	No hay error
1	Not-connected	Todavía no existe un conexión de control para este par PAC-PNS
2	Bad-Format	La longitud es errónea o el valor de la *Magic Cookie* es incorrecto
3	Bad-Value	Uno de los valores de algún campo está fuera de rango o un campo reservado no está en ceros
4	No-Resource	Recursos insuficientes para manejar este comando
5	Bad-Call-ID	El identificador de llamada es incorrecto
6	PAC-Error	Un error específico ocurrió en el PAC

Ilustración 11 Códigos de Error en PPTP

2.3.4.2 Túneles en PPTP: PPTP requiere del establecimiento de un túnel para la comunicación entre una pareja PAC-PNS. Los datos de usuario que transporta PPTP son tramas PPP, las cuales son encapsuladas utilizando GRE. El túnel es utilizado para transportar todas las tramas PPP que pertenecen a una sesión entre una pareja PAC-PNS. Una clave presente en la cabecera GRE indica a cual sesión pertenece una determinada trama PPP. De esta manera, Las tramas PPP son transportadas por rutas distintas pero dentro de un único túnel. [39]

2.3.4.3 Encapsulación Genérica para Ruteo (GRE, Generic Routing Encapsulation): Es un protocolo para encapsular cualquier protocolo de la capa de red dentro de cualquier otro protocolo de la capa de red. El GRE es normalmente utilizado también para servicios VPN. GRE no posee mecanismos de seguridad y debe ser combinado por ejemplo con IPSec para que los datos viajen seguros[40]

La cabecera GRE usado en PPTP se ha mejorado ligeramente respecto a la especificada en el protocolo original GRE. La principal diferencia consiste en la definición de un nuevo campo llamado Número de

39 RFC 2637 Point-to-Point Tunneling Protocol (PPTP)

40 RFC 2784 Generic Routing Encapsulation (GRE)

Reconocimiento, utilizado para determinar si un paquete GRE particular o un conjunto de paquetes han llegado en el extremo remoto del túnel. Esta capacidad de acuse de recibo no se utiliza en conjunción con cualquier retransmisión de paquetes de datos de usuario. Se utiliza para determinar la velocidad a la que los paquetes de datos de usuario han de ser transmitidos a través del túnel para una sesión de usuario dado. El formato de la cabecera GRE mejorada es como se muestra en la siguiente figura:

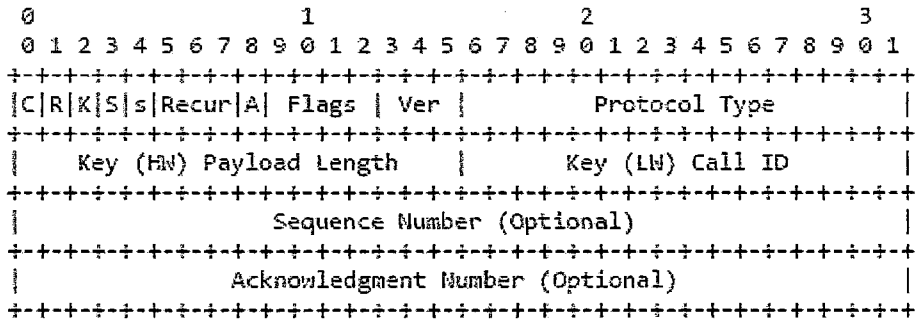


Ilustración 12 Cabecera GRE mejorada

La cabecera GRE es descrita a continuación:

- C indica chequeo de suma presente. Se establece en 0.
- R indica ruteo presente. Se establece en 0.
- K indica clave presente. Se establece en 1.
- S indica número de secuencia presente. Se establece en 1 si un paquete de datos está presente, de lo contrario se establece en 0.
- s indica ruta de fuente estricta. Se establece en 0.
- Recur indica control de la recursión. Se establece en 0.
- A indica número de secuencia de reconocimiento presente. Se establece en 1 si el paquete contiene número de reconocimiento para ser usado en el reconocimiento de tramas previamente transmitidas.
- Banderas siempre están en 0.

- Versión siempre está en 1.
- Tipo de protocolo se establece en 880B hexadecimal.
- Clave (HW) indica tamaño de la carga útil.
- Clave (LW) contiene el indicador de llamada para la sesión a la cual pertenece el paquete.
- Número de secuencia contiene el número de secuencia de la carga útil. Presente si S está en 1.
- Número de reconocimiento contiene el número del paquete GRE con el número más grande recibido durante la sesión. Presente si A está en 1. 41

2.3.5 Seguridad en PPTP: PPTP por sí solo no proporciona ningún mecanismo de seguridad. Si los datos que atraviesan el túnel no son cifrados, cualquier usuario no autorizado puede apropiarse de la información. PPTP requiere de protocolos adicionales para poder autenticar usuarios y encriptar la información.

2.3.5.1 Autenticación y control de acceso: Un servidor PPTP actúa como una puerta de enlace a una VPN, es decir, se encarga de controlar todo el acceso a una VPN. La autenticación de los clientes remotos PPTP se realiza utilizando los métodos de autenticación de PPP. Los protocolos de autenticación que usa PPP son CHAP, MS-CHAP y PAP. En los sistemas Windows los clientes PPTP deben proporcionar un nombre de usuario y una clave para poder ser autenticados.

En cuanto a las cuentas de los usuarios, éstas son almacenadas en un directorio del servidor Windows y son administradas a través del administrador de usuarios para dominios, lo cual proporciona una administración centralizada. Sólo las cuentas que tienen permiso de acceso a la VPN a través de un dominio confiable son permitidas. Se requiere de una administración muy cuidadosa de las cuentas para reducir lo más posible los riesgos en la seguridad.

Después de la autenticación, todo el acceso a una LAN privada debe seguir un modelo de seguridad estricto. Todo acceso a los recursos de la red debe de tener los permisos apropiados.

41 RFC 2637 Point-to-Point Tunneling Protocol (PPTP)

Debido a problemas de seguridad que ha tenido PPTP, se ha incluido el uso de EAP para la autenticación. EAP mejora notablemente la seguridad de las VPN basadas en PPTP. Una ventaja de PPTP es que no requiere del uso de una PKI, sin embargo, EAP requiere de certificados digitales para la autenticación mutua y así elevar la seguridad al máximo. [42]

2.3.5.2 Cifrado de datos: PPTP utiliza para cifrar los datos el cifrado MPPE (Microsoft Point to Point Encryption). MPPE es un protocolo de cifrado simétrico que utiliza un algoritmo de cifrado propietario comercializado por RSA Data Security. Este protocolo se llama RSA (Rivest-Shamir-Adleman) RC4 (River Cipher 4). No se trata de un algoritmo patentado pero está protegido como secreto de fabricación (aunque fue divulgado por Internet). Para implementar el cifrado MPPE, es preciso que la autenticación efectuada por PPP sea MS-CHAPv1, MS-CHAPv2 o EAP-TLS. MPPE puede utilizarse con un nivel de cifrado de 40 bits, 56 bits o 128 bits.[43]

2.3.5.3 Filtrado de paquetes PPTP: El filtrado de paquetes PPTP es una característica muy importante. El administrador de red puede decidir que sólo los usuarios PPTP tengan permiso de conectarse a la red corporativa a través de Internet. Todos los paquetes que no son PPTP son filtrados lo que evita el riesgo de que alguien ataque la VPN a través del servidor PPTP. Cuando el filtro de paquetes PPTP es activado, el servidor PPTP de la VPN acepta y enruta sólo los paquetes de usuarios autenticados. Esto evita que todos los demás paquetes que no son PPTP puedan ingresar a la VPN. Esto asegura que sólo los datos cifrados autorizados entran y salen de la LAN privada.

2.3.5.4 Utilizar PPTP con firewalls y routers: El tráfico PPTP utiliza el puerto TCP 1723, y el protocolo IP utiliza el ID 47, de acuerdo a la IANA. PPTP puede ser utilizado en la mayoría de los firewalls y routers al activar el tráfico destinado al puerto 1723 para que sea enrutados a través del firewall o router.

---

42 WindowSecurity-Comparing VPN Options

43 ISA Server 2000 proxy y firewall: optimizar el acceso a internet y la seguridad de la red de la empresa - Philippe Mathon - Ediciones ENI 2002, Página 248

Los firewalls protegen la seguridad de una red empresarial a regular de forma estricta los datos que llegan a la VPN a través de Internet. Una organización puede desplegar un servidor Windows PPTP detrás del firewall. El servidor PPTP acepta los paquetes PPTP que llegan del exterior a través del firewall y extraer la trama PPP del datagrama IP, descifrar el paquete y enviarlo a la computadora destino dentro de la VPN.

CAPÍTULO III

ANÁLISIS Y LEVANTAMIENTO DE RED

CAPÌTULO III

ANÁLISIS Y LEVANTAMIENTO DE RED

3.1 Necesidad del Sistema

El área de soporte de la empresa tiene a su cargo el mantenimiento preventivo y correctivo de las soluciones implementadas en las distintas municipalidades, los cuales se rigen por el contrato de soporte SLA 24x7 firmado con las mismas durante el proceso de implementación de dichas soluciones.

Con respecto al mantenimiento preventivo, se tiene programada dos visitas on site al año, en la cual se incluye un ingeniero a cargo de la revisión de la configuración de todos los equipos y un técnico para la revisión del hardware y conexiones de los dispositivos.

El problema se presenta cuando se implementa los mantenimientos correctivos puesto que estos son reportados por el área usuaria, y como ellos no cuentan con especialistas en el tema, dichos reportes son demasiado genéricos y carecen de la información mínima necesaria para un correcto pre-diagnóstico, obligando así a la empresa a ir a sitio sin las herramientas y personal específico para la solución del problema y en vez de ello lo único que se consigue es realizar un correcto diagnóstico y recién con este resultado tener que regresar con las herramientas y personal adecuado, lo cual genera retrasos y con ello salirnos de los tiempos de respuesta establecidos en los SLA, dejando así una mala imagen de la empresa.

3.2 Análisis de Red

Las redes en las distintas municipalidades están implementadas con sistemas punto a punto que brindan interconexión a las distintas estaciones (cámaras) mediante el uso de equipamiento Inalámbrico. La solución contempla una interconexión inalámbrica utilizando el espectro radioeléctrico, en la banda de 5.150 – 5.850GHz, con velocidades de hasta 300 Mbps, los enlaces punto a punto transportan las señales digitales de video provenientes de las cámaras de video vigilancia hasta los Nodos, dispuestas en una "Topología de Transmisión en Estrella". Así pues las señales de las estaciones confluyen a los Nodos de su radio de cobertura y estos a su vez se encargarán de transportar la señal concentrada en ellos hasta el Nodo Principal – Centro de Control y Monitoreo (CCM).

3.2.1 Descripción de equipos y número de enlaces en las distintas Municipalidades:

La siguiente tabla muestra el equipamiento con el cual se encuentran dotados los sistemas de video vigilancia de cada municipalidad. La siguiente tabla es de suma importancia para poder identificar los elementos que conformarán nuestro sistema de monitoreo y gestión y así conocer su naturaleza para poder listar los parámetros que deseamos monitorear y conocer los tipos de acceso que necesitamos para su integración al sistema.

	Equipos		N° de Enlaces
	Descripción	N°	
M. Rímac	Cámaras HD Domo IP PTZ Bosch Auto dome VG5	18	21
	Cámaras Fijas	02	
	Sistema de UPS con autonomía de 60 Minutos Blazer Vista	18	
	Radioenlace PTP de Alta Capacidad AIR BR600ANH (Interconexión de Nodos)	06	
	Radioenlace PTP de Última Milla AIR PTP600L (Interconexión de Cámaras HD Domo IP PTZ)	36	
	Antenas Direccionales Parabólicas Sólidas para Enlaces Nodo W5G 30D-DP	06	
	Switch de 24 Puertos Capa 3 DLINK DGS-3627	04	
M. San Juan de Lurigancho	Cámaras DOMO IP PTZ Bosch VG4	16	18
	Cámaras Fijas	02	
	Sistema de UPS con autonomía de 60 Minutos Blazer Vista	16	

	Radio Enlace PTP MB-ROMBv4 (Interconexión de Cámaras HD Domo IP PTZ e Interconexión de Nodos)	36	
	Antenas Hyperlink tipo grilla de 25dBi	32	
	Antenas Direccionales Parabólicas Sólidas para Enlaces Nodo W5G 30D-DP	04	
	Switch HP ProCurve 2610-48	03	
M. Cuzco	Cámaras DOMO IP PTZ Bosch VG4	21	22
	Sistema de UPS con autonomía de 60 Minutos Blazer Vista	21	
	Radio Enlace PTP MB-ROMBv4 (Interconexión de Cámaras HD Domo IP PTZ e Interconexión de Nodos)	44	
	Antena W5G-29D 4.9 to 5.8GHz Wideband 29dBi Parabolic Dish Antenna	2	
	Antenas Hyperlink tipo grilla de 25dBi	42	
	Switch D'link modelo DXS-3350SR	2	
M. Piura	Cámaras DOMO IP PTZ Bosch VG4	53	57
	Sistema de UPS con autonomía de 60 Minutos Blazer Vista	53	
	Antenas Hyperlink tipo grilla de 25dBi	114	
	Radio Enlace PTP MB-ROMBv4 (Interconexión de Cámaras HD Domo IP PTZ e Interconexión de Nodos)	114	
	Switch de 24 Puertos Capa 3 DLINK DGS-3627	5	
M. Castilla	Cámaras Domo IP PTZ Bosch Auto dome 800 HD	21	24
	Cámaras Fijas Bosh	01	
	Sistema de UPS con autonomía de 60 Minutos Blazer Vista	21	
	Radio PTP UBIQUITY NBM5-22DBI	42	
	Radio BackHaul UBIQUITY Power Bridge	06	
	SWITCH L3 HP 2620-24	04	

Tabla 2 Descripción de Equipos y Número de Enlaces

3.2.2 Topologías de Red por Municipalidad

A continuación se muestra la distribución de los enlaces punto a punto de cada una de las municipalidades. Dichas topologías fueron creadas por los autores después de una recopilación de información en campo.

- Red de Cámaras Municipalidad del RIMAC

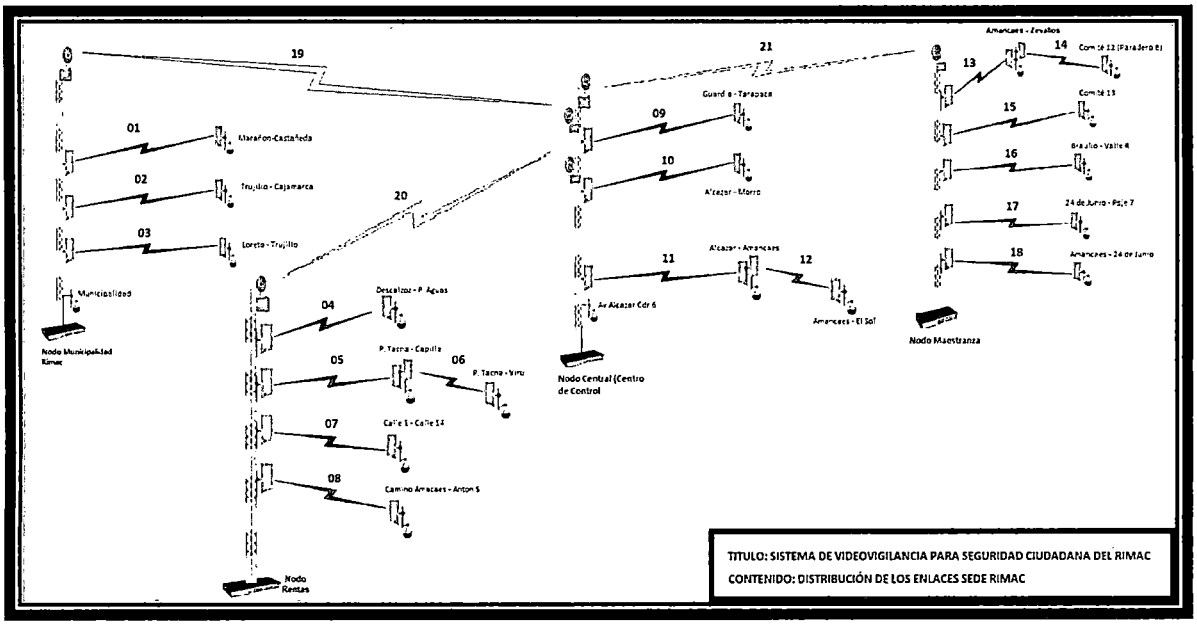


Ilustración 13 Topología Sistema CCTV Rímac

- Red de Cámaras Municipalidad de San Juan de Lurigancho

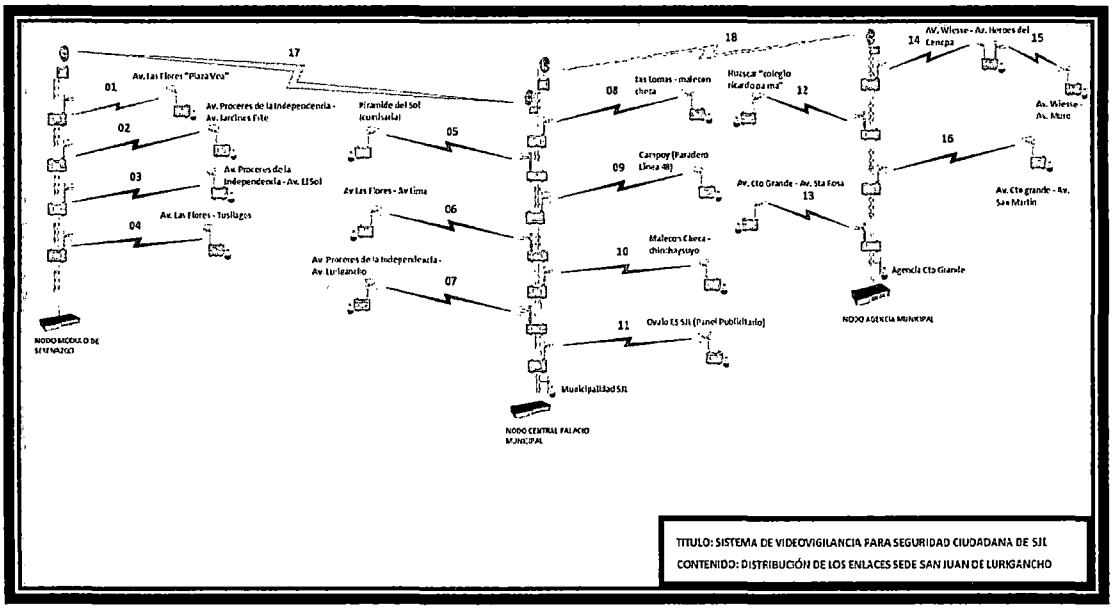


Ilustración 14 Topología Sistema CCTV San Juan de Lurigancho

- Red de Cámaras Municipalidad Cusco

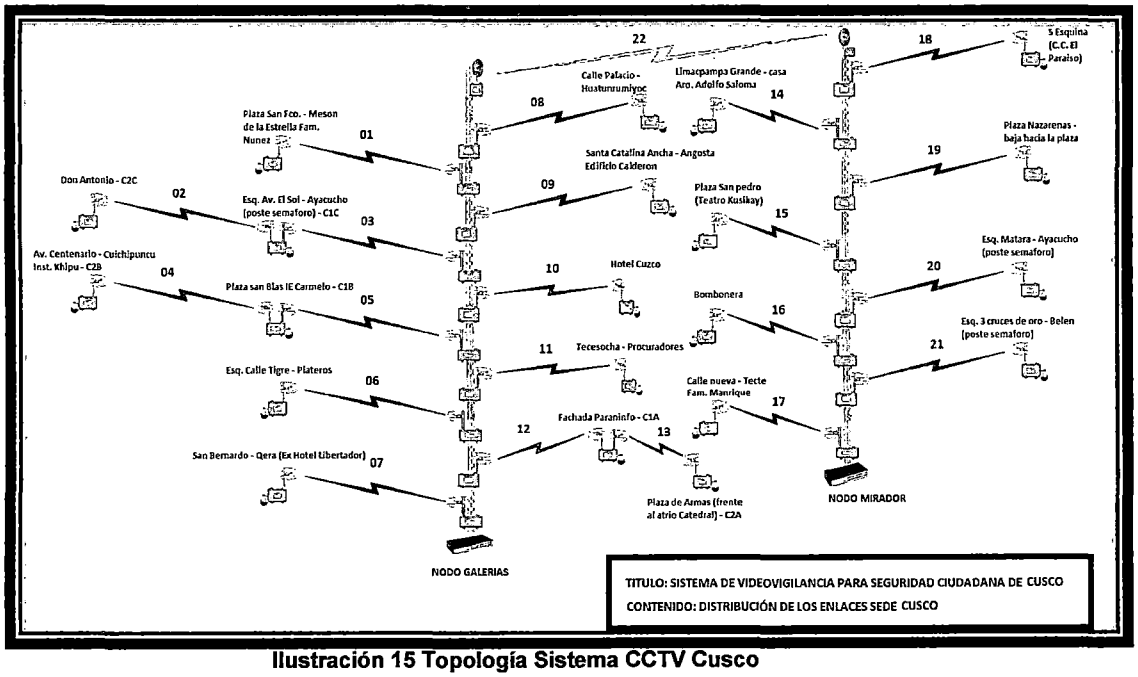


Ilustración 15 Topología Sistema CCTV Cusco

- Red de Cámaras Municipalidad de Castilla

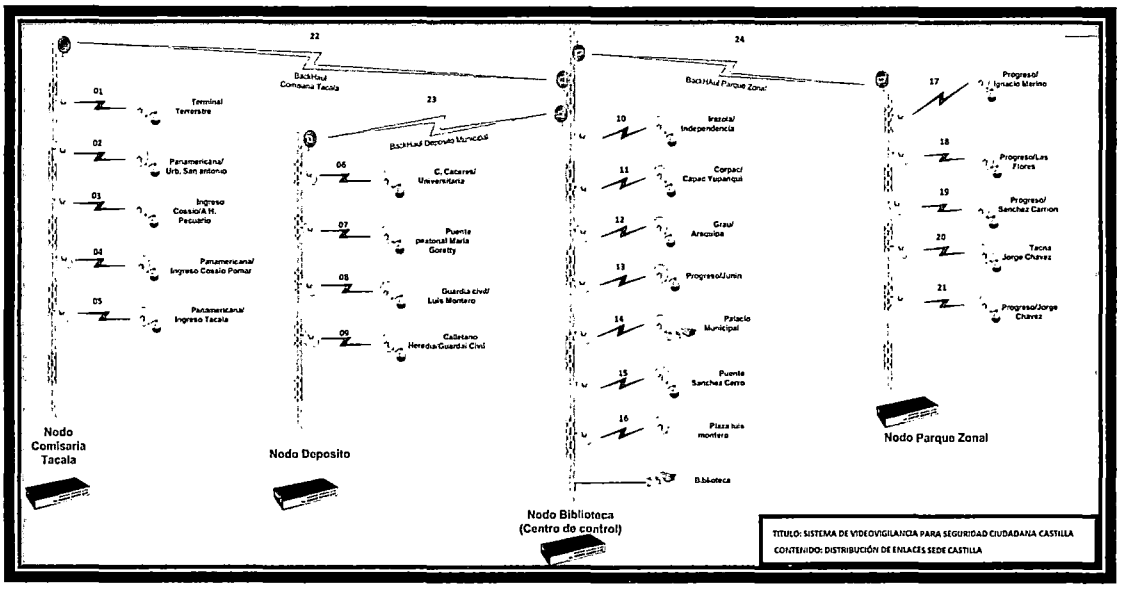


Ilustración 16 Topología Sistema CCTV Castilla

- Red de Cámaras Municipalidad de Piura

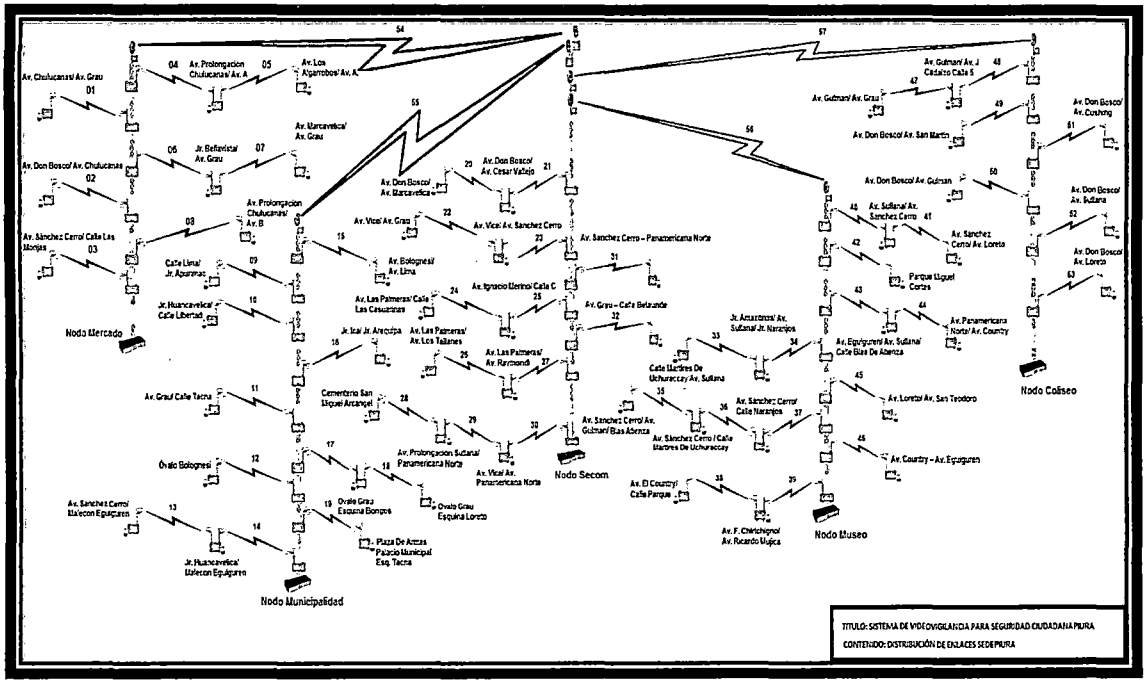


Ilustración 17 Topología Sistema CCTV Piura

3.2.3 Tablas de Direccionamiento IP de Enlaces

En las siguientes tablas recopilamos la información sobre las direcciones IP de todos los dispositivos pertenecientes a las redes de cada municipalidad. Esta información nos será de suma importancia en el momento de crear nuestros mapas de red en el NMS, esto se detalla en los capítulos posteriores.

- Municipalidad del Rímac

Enlace	Ubicación	Dirección IP Cámara	IP Radio Poste	IP Radio Nodo	Nodo
1	Jr. Marañón / Jr. Castañeta	172.172.10.4	172.172.10.3	172.172.10.2	MUNICIPAL
2	Jr. Cajamarca / Jr. Trujillo	172.172.30.4	172.172.30.3	172.172.30.2	
3	Jr. Loreto / Jr. Trujillo	172.172.20.4	172.172.20.3	172.172.20.2	
4	Descalzos / Paseo de Aguas	172.172.50.4	172.172.50.3	172.172.50.2	RENTAS
5	Prolog. Tacna / Av. La Capilla	172.172.70.4	172.172.70.3	172.172.70.2	
6	Prolog. Tacna / Jr. Virú	172.172.70.7	172.172.70.6	172.172.70.5	
7	Calle 1 (Av. Cajetambo) / Calle 14	172.172.80.4	172.172.80.3	172.172.80.2	
8	Av. Amancaes/Av. A. Sánchez	172.172.60.4	172.172.60.3	172.172.60.2	
9	Av. Guardia Peruana/ Av. Tarapacá	172.172.170.4	172.172.170.3	172.172.170.2	CENTRAL
10	Av. alcázar / Av. Morro de Arica	172.172.180.4	172.172.180.3	172.172.180.2	
11	Av. Amancaes / Av. Alcázar	172.172.160.4	172.172.160.3	172.172.160.2	
12	Av. Amancaes /Av. El Sol	172.172.160.7	172.172.160.6	172.172.160.5	
-	Av. Alcazar Cdra.6	172.172.9.4	-	-	
13	Av. Amancaes / Horacio Zevallos	172.172.130.4	172.172.130.3	172.172.130.2	MAESTRANZA
14	Comité 12 Ref: Pdro. Inicial Línea B	172.172.130.7	172.172.130.6	172.172.130.5	
15	Av. Flor de Amancaes / Comité 13	172.172.120.4	172.172.120.3	172.172.120.2	
16	Av. B. Sancho Dávila/ Ca.Valle Riestra	172.172.110.4	172.172.110.3	172.172.110.2	

17	Av. 24 de Junio / Psje. 7	172.172.100.4	172.172.100.3	172.172.100.2	
18	Av. Amancaes / Av. 24 de Junio	172.172.90.4	172.172.90.3	172.172.90.2	

Tabla 3 Direccionamiento IP M. Rímac

Enlace	Backhauld	IP Nodo Central	IP Nodo Remoto
19	Nodo Municipalidad/ Nodo Central de Monitoreo	172.192.10.2	172.192.10.3
20	Nodo Rentas/ Nodo Central de Monitoreo	172.192.20.2	172.192.20.3
21	Nodo Maestranza/ Nodo Central de Monitoreo	172.192.30.2	172.192.30.3

Tabla 4 Direccionamiento del Backhauld M. Rímac

- Municipalidad de San Juan de Lurigancho

Enlace	Ubicación	Dirección IP Cámara	IP Radio Poste	IP Radio Nodo	Nodo
1	Av. Las Flores "Plaza Vea"	172.27.4.4	172.27.4.3	172.27.4.2	SERENAZGO
2	Av. Próceres de la Independencia/ Av. Jardines Este	172.27.3.4	172.27.3.3	172.27.3.2	
3	Av. Próceres de la Independencia/ Av. El Sol	172.27.5.4	172.27.5.3	172.27.5.2	
4	Av. Las Flores/ Tusilagos	172.27.2.4	172.27.2.3	172.27.2.2	
5	Pirámide del Sol (comisaria)	172.25.2.4	172.25.2.3	172.25.2.2	PALACIO MUNICIPAL
6	Av. Las Flores/ Av. Lima	172.25.4.4	172.25.4.3	172.25.4.2	
7	Av. Próceres de la Independencia/ Av. Lurigancho	172.25.6.4	172.25.6.3	172.25.6.2	
8	Las Lomas/ malecón checa	172.25.5.4	172.25.5.3	172.25.5.2	
9	Campoy (Paradero Línea 48)	172.25.5.7	172.25.5.6	172.25.5.5	
10	Malecón Checa/ chinchaysuyo	172.25.1.4	172.25.1.3	172.25.1.2	
11	Ovalo ES SJL (Panel Publicitario)	172.25.3.4	172.25.3.3	172.25.3.2	

12	Huáscar "colegio Ricardo palma"	172.26.4.4	172.26.4.3	172.26.4.2	AGENCIA
13	Av. Cto Grande/ Av. Sta. Rosa	172.26.1.4	172.26.1.3	172.26.1.2	
14	Av. Wiesse/ Av. Muro	172.26.2.7	172.26.2.6	172.26.2.5	
15	AV. Wiesse/ Av. Héroes del Cenepa	172.26.2.4	172.26.2.3	172.26.2.2	
16	Av. Cto grande/ Av. San Martin	172.26.3.4	172.26.3.3	172.26.3.2	
-	Municipalidad SJL	172.25.5.7	-	-	
-	Agencia Cto Grande	172.26.1.5	-	-	

Tabla 5 Direccionamiento IP M. San Juan de Lurigancho

Enlace	Backhauld	IP Nodo Central	IP Nodo Remoto
17	Nodo Serenazgo / Nodo Palacio Municipal	172.20.200.2	172.20.200.3
18	Nodo Agencia Municipal / Nodo Palacio Municipal	172.20.100.2	172.20.100.3

Tabla 6 Direccionamiento IP del Backhauld M. San Juan de Lurigancho

- Municipalidad de Cuzco

Enlace	Ubicación	Dirección IP Cámara	IP Radio Poste	IP Radio Nodo	Nodo
1	San Fco. Y Mesón de la Estrella Fam. Nunez	20.20.108.4	20.20.108.3	20.20.108.2	GALERIAS
2	Don Antonio - C2C	20.20.109.7	20.20.109.6	20.20.109.5	
3	Esq. Av. El Sol y Ayacucho (poste semáforo)	20.20.109.4	20.20.109.3	20.20.109.2	
4	Av. Centenario y Cuichipuncu Inst. Khipu - C2B	20.20.104.7	20.20.104.6	20.20.104.5	
5	Plaza san Blas IE Carmelo - C1B	20.20.104.4	20.20.104.3	20.20.104.2	
6	Esq. Calle Tigre y Plateros	20.20.102.4	20.20.102.3	20.20.102.2	
7	San Bernardo / Qera (Ex Hotel Libertador)	20.20.106.4	20.20.106.3	20.20.106.2	
8	Calle Palacio y	20.20.103.4	20.20.103.3	20.20.103.2	

	Huatunrumiyoc				
9	Santa Catalina Ancha y Angosta Edificio Calderón	20.20.110.4	20.20.110.3	20.20.110.2	
10	Hotel Cuzco	20.20.105.4	20.20.105.3	20.20.105.2	
11	Tecesocha - Procuradores	20.20.101.4	20.20.101.3	20.20.101.2	
12	Fachada Paraninfo - C1A	20.20.100.4	20.20.100.3	20.20.100.2	
13	Plaza de Armas (frente al atrio Catedral) - C2A	20.20.100.7	20.20.100.6	20.20.100.5	
14	Limacpampa Grande y casa Arq. Adolfo Saloma	10.10.103.4	10.10.103.3	10.10.103.2	MIRADOR
15	Plaza San pedro (Teatro Kusikay)	10.10.104.4	10.10.104.3	10.10.104.2	
16	Bombonera	10.10.100.4	10.10.100.3	10.10.100.2	
17	Calle nueva y Tecte Fam. Manrique	10.10.108.4	10.10.108.3	10.10.108.2	
18	Esquina (C.C. El Paraíso)	10.10.106.4	10.10.106.3	10.10.106.2	
19	Plaza Nazarenas y baja hacia la plaza	10.10.101.4	10.10.101.3	10.10.101.2	
20	Esq. Matara y Ayacucho (poste semáforo)	10.10.102.4	10.10.102.3	10.10.102.2	
21	Esq. 3 cruces de oro y Belén (poste semáforo)	10.10.105.4	10.10.105.3	10.10.105.2	

Tabla 7 Direccionamiento IP M. Cusco

Enlace	Ubicación	IP Nodo Central	IP Nodo Remoto
22	Nodo Galerías a Nodo Mirador	172.192.10.2	172.192.10.3

Tabla 8 Direccionamiento IP del Backhauld M. Cusco

- Municipalidad de Castilla

Enlace	Ubicación	Dirección IP Cámara	IP Radio Poste	IP Radio Nodo	Nodo
1	Terminal Terrestre Castilla	192.100.4.4	192.100.4.3	192.100.4.2	COMISARIA
2	Av. Panamericana / Urb. San Antonio	192.100.12.4	192.100.12.3	192.100.12.2	
3	Ingreso Cossio del Pomar/ A.H. Pecuario Nuevo Horizonte	192.100.16.4	192.100.16.3	192.100.16.2	
4	Av. Panamericana/ Ingreso AA.HH. Cosillo Pomar	192.100.15.4	192.100.15.3	192.100.15.2	
5	Av. Panamericana / AA.HH. Ingreso Tácala	192.100.14.4	192.100.14.3	192.100.14.2	
6	Av. Andrés A. Cáceres / Av. Universitaria	192.100.1.4	192.100.1.3	192.100.1.2	DEPOSITO
7	Puente Peatonal / AA.HH. - María Goretty	192.100.11.4	192.100.11.3	192.100.11.2	
8	Guardia Civil / Luis Montero	192.100.9.4	192.100.9.3	192.100.9.2	
9	Av. Cayetano Heredia / Guardia Civil	192.100.3.4	192.100.3.3	192.100.3.2	
10	Av. Irazola/ Av. Independencia	192.100.8.4	192.100.8.3	192.100.8.2	BIBLIOTECA
11	Av. Corpac / Av. Capac Yupanqui	192.100.13.4	192.100.13.3	192.100.13.2	
12	Av. Grau / Av. Arequipa	192.100.10.4	192.100.10.3	192.100.10.2	
13	Av. Progreso / Av. Junín	192.100.2.4	192.100.2.3	192.100.2.2	
14	Palacio Municipal	192.100.22.4	192.100.22.3	192.100.22.2	
15	Puente Sánchez Cerro	192.100.6.4	192.100.6.3	192.100.6.2	
16	Plaza Luis Montero	192.100.7.4	192.100.7.3	192.100.7.2	
-	Cámara Fija Nodo Biblioteca	172.100.21.4	-	-	
17	Av. Progreso / Ignacio Merino	192.100.20.4	192.100.20.3	192.100.20.2	PARQUE ZONAL
18	Av. Progreso / Av. Las Flores	192.100.17.4	192.100.17.3	192.100.17.2	
19	Av. Progreso / Av. Sánchez Carrión	192.100.18.4	192.100.18.3	192.100.18.2	
20	Av. Tacna / Jorge Chávez	192.100.5.4	192.100.3.3	192.100.5.5	

21	Av. Progreso / Av. Jorge Chávez	192.100.19.4	192.100.19.3	192.100.19.2	

Tabla 9 Direccionamiento IP M. Castilla

Enlace	Backhauld	IP Nodo Central	IP Nodo Remoto
22	Nodo Comisaria Tacala / Nodo Central	172.100.31.3	172.100.31.2
23	Nodo Deposito / Nodo Central	172.100.32.3	172.100.32.2
24	Nodo Parque Zonal / Nodo Central	172.100.33.3	172.100.33.2

Tabla 10 Direccionamiento IP del Backhauld M. Castilla

- Municipalidad de Piura

Enlace	Ubicación	Dirección IP Cámara	IP Radio Poste	IP Radio Nodo	Nodo
1	Av. Chulucanas / Av. Grau	172.24.4.4	172.24.4.3	172.24.4.2	Mercado
2	Av. Don Bosco / Av. Chulucanas	172.24.1.4	172.24.1.3	172.24.1.2	
3	Av. Sánchez Cerro / Calle Las Monjas	172.24.6.4	172.24.6.3	172.24.6.2	
4	Av. Prolongación Chulucanas / Av. A	172.24.5.4	172.24.5.3	172.24.5.2	
5	Av. Los Algarrobos / Av. A.	172.24.5.7	172.24.5.6	172.24.5.5	
6	Jr. Bellavista / Av. Grau	172.24.3.4	172.24.3.3	172.24.3.2	
7	Av. Marcavelica / Av. Grau	172.24.3.7	172.24.3.6	172.24.3.5	
8	Av. Av. Prolongación Chulucanas / Av. B	172.24.2.4	172.24.2.3	172.24.2.2	
9	Calle Lima / Jr. Apurímac	172.23.4.4	172.23.4.3	172.23.4.2	Municipalidad
10	Jr. Huancavelica / Calle Libertad	172.23.5.4	172.23.5.3	172.23.5.2	
11	Av. Grau / Calle Tacna	172.23.7.4	172.23.7.3	172.23.7.2	
12	Óvalo Bolognesi	172.23.3.4	172.23.3.3	172.23.3.2	
13	Av. Sánchez Cerro / Malecón Eguren	172.23.1.7	172.23.1.6	172.23.1.5	
14	Jr. Huancavelica / Malecón Eguren	172.23.1.4	172.23.1.3	172.23.1.2	
15	Av. Bolognesi / Av. Lima / Malecón Eguren	172.23.8.4	172.23.8.3	172.23.8.2	
16	Jr. Ica / Jr. Arequipa	172.23.6.4	172.23.6.3	172.23.6.2	

17	Ovalo Grau Esquina Bongos Agencia Interbank	172.23.9.4	172.23.9.3	172.23.9.2	
18	Ovalo Grau Esquina Loreto	172.23.2.4	172.23.2.3	172.23.2.2	
19	Plaza De Armas Palacio Municipal Esq. Tacna	172.23.10.4	172.23.10.3	172.23.10.2	
20	Av. Don Bosco / Av. Marcavelica	172.21.2.7	172.21.2.6	172.21.2.5	Secom
21	Av. Don Bosco / Av. Cesar Vallejo	172.21.2.4	172.21.2.3	172.21.2.2	
22	Av. Vice / Av. Grau	172.21.6.7	172.21.6.6	172.21.6.5	
23	Av. Vice / Av. Sánchez Cerro	172.21.6.4	172.21.6.3	172.21.6.2	
24	Av. Las Palmeras / Calle Las Casuarinas	172.21.5.7	172.21.5.6	172.21.5.5	
25	Av. Ignacio Merino / Calle C	172.21.5.4	172.21.5.3	172.21.5.2	
26	Av. Las Palmeras / Av. Los Tallanes	172.21.1.7	172.21.1.6	172.21.1.5	
27	Av. Las Palmeras / Av. Raymondi	172.21.1.4	172.21.1.3	172.21.1.2	
28	Av. Panamericana Frente A Cementerio San Miguel Arcángel	172.21.7.10	172.21.7.9	172.21.7.8	
29	Av. Prolongación Sullana / Panamericana Norte	172.21.7.7	172.21.7.6	172.21.7.5	
30	Av. Vice / Av. Panamericana Norte	172.21.7.4	172.21.7.3	172.21.7.2	
31	Av. Sánchez Cerro / Panamericana Norte	172.21.4.4	172.21.4.3	172.21.4.2	
32	Av. Grau / Calle Belaunde	172.21.3.4	172.21.3.3	172.21.3.2	
33	Calle mártires De Uchuraccay / Av. Sullana	172.25.10.4	172.25.10.3	172.25.10.2	Museo
34	Jr. Amazonas / Av. Sullana / Jr. Naranjos	172.25.11.4	172.25.11.3	172.25.11.2	
35	Av. Sánchez Cerro / Av. Gulman / Blas Atienza	172.25.7.10	172.25.7.9	172.25.7.8	
36	Av. Sánchez Cerro / Calle Mártires De Uchuraccay	172.25.7.7	172.25.7.6	172.25.7.5	
37	Av. Sánchez Cerro / Calle Naranjos	172.25.7.4	172.25.7.3	172.25.7.2	
38	Av. El Country / Calle Parque	172.25.12.7	172.25.12.6	172.25.12.5	

39	Av. F. Chirichigno / Av. Ricardo Mujica	172.25.12.4	172.25.12.3	172.25.12.2	
40	Av. Sullana / Av. Sánchez Cerro	172.25.8.4	172.25.8.3	172.25.8.2	
41	Av. Sánchez Cerro / Av. Loreto	172.25.8.7	172.25.8.6	172.25.8.5	
42	Parque Miguel Cortes	172.25.6.4	172.25.6.3	172.25.6.2	
43	Av. Eguren / Av. Sullana / Calle Blas De Atienza	172.25.13.4	172.25.13.3	172.25.13.2	
44	Av. Panamericana Norte / Av. Country	172.25.13.7	172.25.13.6	172.25.13.5	
45	Av. Loreto / Av. San Teodoro	172.25.14.4	172.25.14.3	172.25.14.2	
46	Av. Country / Av. Eguren	172.25.10.7	172.25.10.6	172.25.10.2	
47	Av. Gulman / Av. Grau	172.22.1.7	172.22.1.6	172.22.1.5	Coliseo
48	Av. Gulman / Av. J Cadalzo Calle 5	172.22.1.4	172.22.1.3	172.22.1.2	
49	Av. Don Bosco / Av. San Martin	172.22.5.4	172.22.5.3	172.22.5.2	
50	Av. Don Bosco / Av. Gulman	172.22.2.4	172.22.2.3	172.22.2.2	
51	Av. Don Bosco / Av. Cushing	172.22.6.4	172.22.6.3	172.22.6.2	
52	Av. Don Bosco / Av. Sullana	172.22.4.4	172.22.4.3	172.22.4.2	
53	Av. Don Bosco / Av. Loreto	172.22.3.4	172.22.3.3	172.22.3.2	

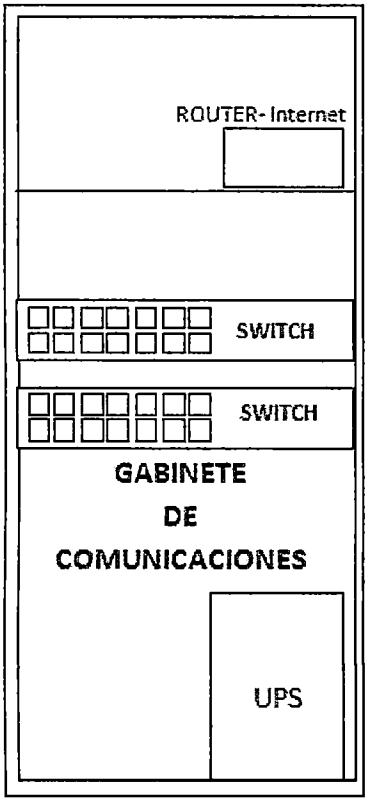
Tabla 11 Direccionamiento IP M. Piura

Enlace	Backhaul	IP Nodo Central	IP Nodo Remoto
54	Nodo Mercado / Nodo Secom	172.26.6.2	172.26.6.3
55	Nodo Municipalidad / Nodo Secom	172.26.7.2	172.26.7.3
56	Nodo Museo / Nodo Secom	172.26.5.2	172.26.5.3
57	Nodo Coliseo / Nodo Secom	172.26.8.2	172.26.8.3

Tabla 12 Direccionamiento IP del Backhauld M. Piura

3.2.4 Distribución de Equipos en el Gabinete Central de Cada Municipalidad

Se coordinó con personal de soporte In-Situ de la empresa Netkrom Technologies la visita al centro de monitoreo de cada municipalidad con la finalidad de obtener la distribución actual de los equipos en el gabinete de comunicaciones. Obteniendo como resultado el siguiente estándar



01 Switch que conecta a todas las computadoras situadas en la sala de observación y sala de crisis del Centro de Monitoreo, al cual llamaremos switch principal.

01 Switch que conecta a todos los equipos de radio situados en la torre del Centro de Monitoreo.

01 Router perteneciente al ISP para la conexión a internet.

01 UPS para protección ante fallas eléctricas

Ilustración 18 Modelo Estándar del Gabinete Principal en los Centros de Monitoreo

3.3 Levantamiento de Red

3.3.1 Topología de Interconexión

Para lograr la interconexión de los centros de monitoreo de cada municipalidad con la sede de la empresa Netkrom se tuvo que implementar un sistema de VPNs sobre las redes existentes en dichas municipalidades, la siguiente imagen muestra la topología final de interconexión.

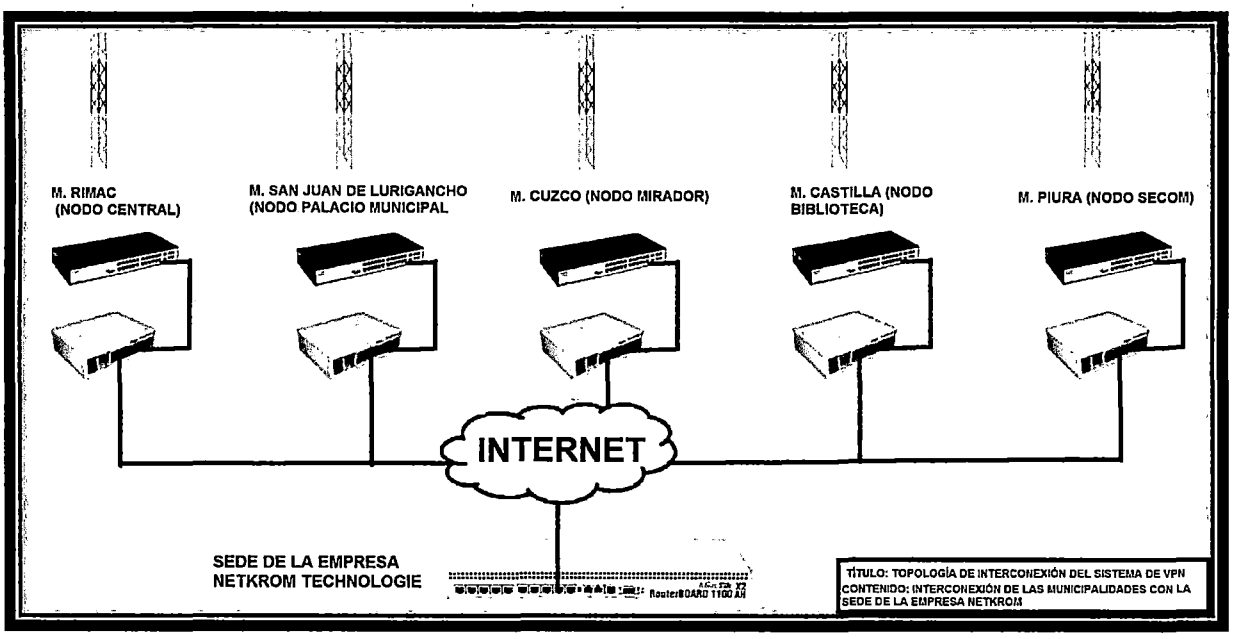


Ilustración 19 Topología de Interconexión del Sistema de VPN

3.3.2 Implementación de Equipos por Municipalidad

A continuación se lista los equipos y accesorios que se implementaron en los diferentes Nodos Centrales de cada Municipalidad, cabe resaltar que en este capítulo solo se mencionan dichos equipos y accesorios puesto que en los capítulos posteriores se detallará la configuración de los mismos. En el Anexo A se encuentra los datasheets de dicho equipamiento.

Municipalidad del Rímac	RouterBoard MIKROTIK 750 GL	01
	Patch Cord CAT5 de 3mts c/u	02
Municipalidad de San Juan de Lurigancho	RouterBoard MIKROTIK 750 GL	01
	Patch Cord CAT5 de 3mts c/u	02
Municipalidad del Cuzco.	RouterBoard MIKROTIK 750 GL	01
	Patch Cord CAT5 de 3mts c/u	02
Municipalidad de Piura.	RouterBoard MIKROTIK 750 GL	01
	Patch Cord CAT5 de 3mts c/u	02
Municipalidad de Castilla.	RouterBoard MIKROTIK 750 GL	01
	Patch Cord CAT5 de 3mts c/u	02

Tabla 13 Listados de Equipos Para Instalación en Las Municipalidades

3.3.3 Implementación de Equipos en la Sede de la Empresa Netkrom

A continuación se detalla los equipos y accesorios que se implementaron para la creación de la VPN servidor y el sistema de Gestión y Monitoreo en la empresa Netkrom Technologies. En el Anexo A se encuentra los datasheets de dicho equipamiento.

Ítem	Descripción	Cantidad
1	RouterBoard MIKROTIK 1100AH x2	01
2	Patch Cord CAT5 de 3mts c/u	06
3	PC HP Compaq 6300 Pro SFF	01
4	Teclado+ Mouse Microsoft Inalámbrico	01
5	Supresor de Picos Forza 220V.	01
6	Estabilizador APC 1200va	01
7	Smart- UPS APC C1000	01
8	Monitores LCD 42" LG	02
9	Cables HDMI 3mts c/u	02
10	Rack de Pared para TV de 42"	02
11	Tarjeta de Video ASUS NVIDIA GeForce GT 630, 2 GB GDDR3, HDMI, DVI. Puerto PCI Express 2.0.	01

Tabla 14 Listados de Equipos Para Instalación en La Empresa Netkrom

3.3.4 Instalación del Router Mikrotik en las Municipalidades.

Se requirió la implementación de un Router Mikrotik RB750GL en cada municipio para lo cual se envió solicitudes a los encargados de dichos centros de Monitoreo vía email, requiriendo la aprobación para la instalación del Router Mikrotik.

Posterior a la aprobación, se coordinó vía telefónica con el personal in situ de empresa Netkrom la instalación correspondiente en cada sede, se pidió que se conecte la primera interfaz del mikrotik con el router proveedor de internet y la segunda interfaz con el Switch principal tal como se muestra en la siguiente imagen.

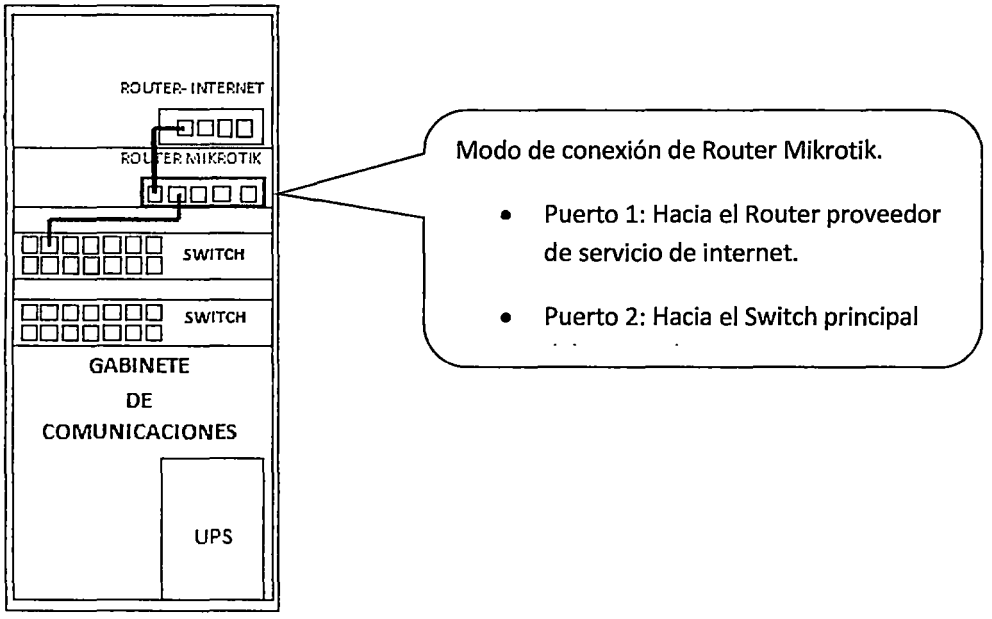


Ilustración 20 Modo de Conexión del Router Mikrotik en los Centros de Monitoreo

3.3.5 Instalación del Equipamiento en la Empresa Netkrom Technologies.

Se realizó la instalación de Router Mikrotik RB1100, donde se configurará el servidor VPN, para lograr la interconexión con las redes de las municipalidades, también se instaló el servidor PC HP Compaq 6300 Pro SFF donde se realizará la instalación del software The Dude, el cual servirá como NMS y será en donde configuraremos nuestros mapas de red y será desde donde se gestionará y monitoreará las redes de las municipalidades y para garantizar su funcionabilidad ante cortes del flujo eléctrico también se instaló un UPS APC 1000VA todo ello lo ubicamos en el data center de la empresa Netkrom Technologies, en la sala del NOC se instalaron 2 pantallas LCD de 42 pulgadas para la visualización de los mapas de red, tal como muestra la siguiente imagen:

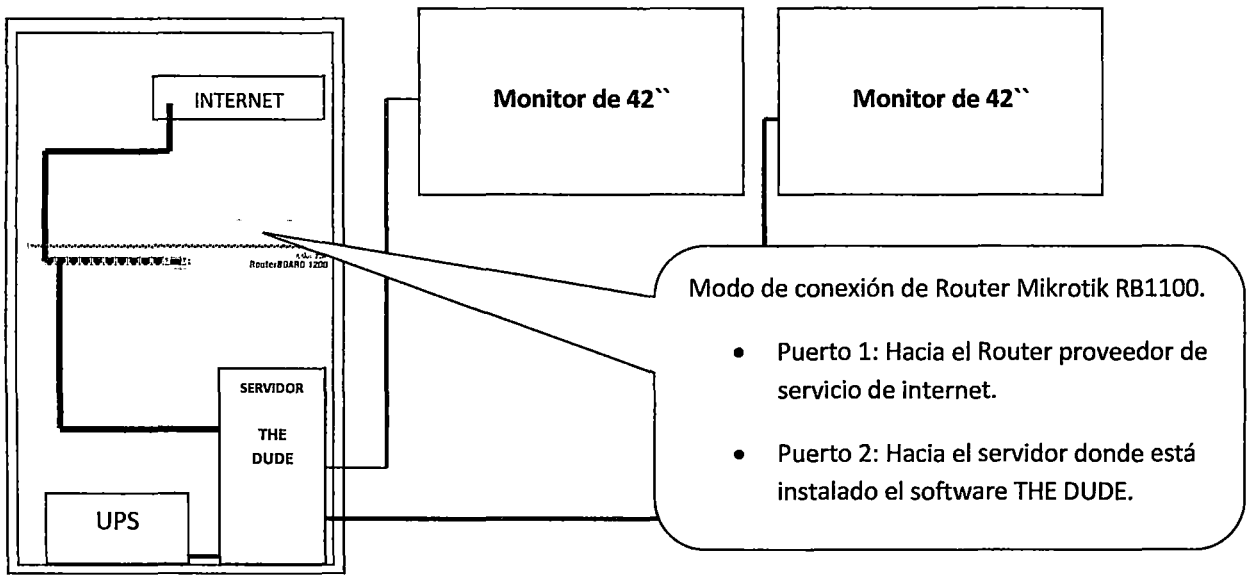


Ilustración 21 Diagrama de Instalación de Router Mikrotik en el Data Center Principal

CAPÍTULO IV

IMPLEMENTACIÓN DEL SISTEMA DE VPN

CAPÍTULO IV

IMPLEMENTACIÓN DEL SISTEMA DE VPN

De acuerdo a la posición geográfica de nuestra muestra el tipo de acceso desde la empresa hacia las municipalidades es remoto por lo cual se creará un sistema de VPNs para lograr su interconexión.

Se seleccionó la tecnología de VPN PPTP tomando en cuenta la basta información encontrada en la red, su fácil implementación, su compatibilidad con los equipos utilizados y debido a su autentificación por usuarios y filtrado de paquetes.

4.1 Implementación de los VPN Cliente

En los nodos centrales de cada Municipalidad se realizaron las siguientes actividades para lograr su interconexión con la sede principal de la empresa:

4.1.1 Apertura de Puerto:

Después de la implementación del Router Mikrotik RB750GL en cada municipio se requirió que se nos brinde un punto de internet (ya sea con una IP privada o Pública), con la apertura del puerto 1723, ya que este puerto es necesario para la creación de la VPN PPTP.

Después que nos confirmaran la apertura nosotros lo corroboramos utilizando la herramienta Open Port, Después de estar seguros de la apertura iniciamos la configuración del mikrotik.

4.1.2 Creación del VPN Cliente en el Router Mikrotik

En este capítulo se describe el procedimiento de la configuración paso a paso de una VPN Cliente en general, en el Anexo B, se muestra las configuraciones realizadas para cada Municipalidad.

a. Para la configuración del Router Mikrotik se descargó la aplicación de configuración llamado Winbox a través de la página web http://download2.mikrotik.com/routeros/winbox/3.0beta3/winbox.exe, se resalta que esta aplicación es un ejecutable y por ende no necesita instalación.

Ilustración 22 Símbolo Winbox

b. Dando doble clic en el ícono Ingresamos a la aplicación Winbox, se abrirá una ventana como se muestra en la figura, clic en los **3 puntos suspensivos**, esto te muestra todos los equipos Mikrotik conectados a la red, en nuestro caso solo aparece el RouterBoard Mikrotik que instalamos anteriormente, seleccionamos este por MAC y damos clic en **Connect**.

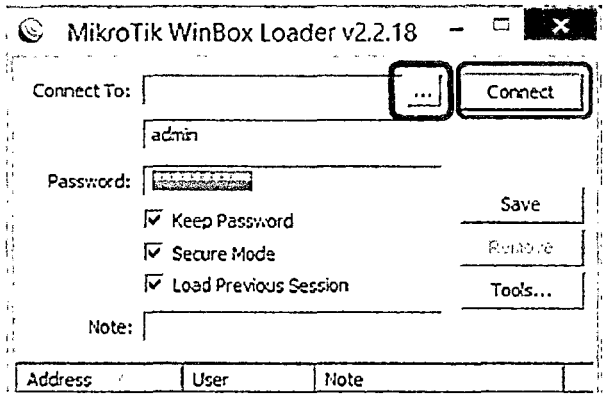


Ilustración 23 Ventana de Inicio Winbox

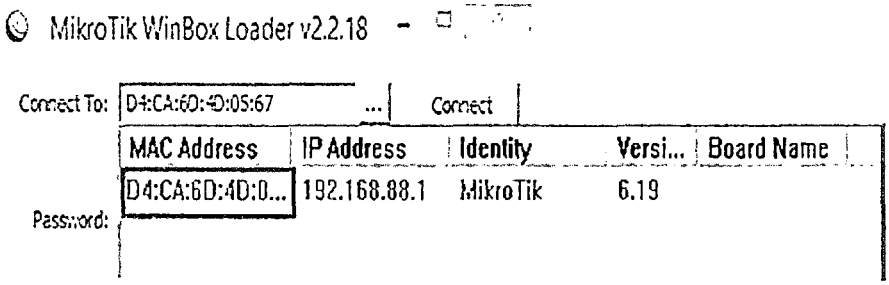


Ilustración 24 Ventana de Conexión Winbox

c. Nos muestra un cuadro de inicio de configuración en el cual hacemos clic en **Remove Configuration**, puesto que vienen con configuraciones por defecto que no son necesarias para nuestro proyecto, posterior a esto el equipo Mikrotik se reinicia, después de ello repetimos el paso anterior.

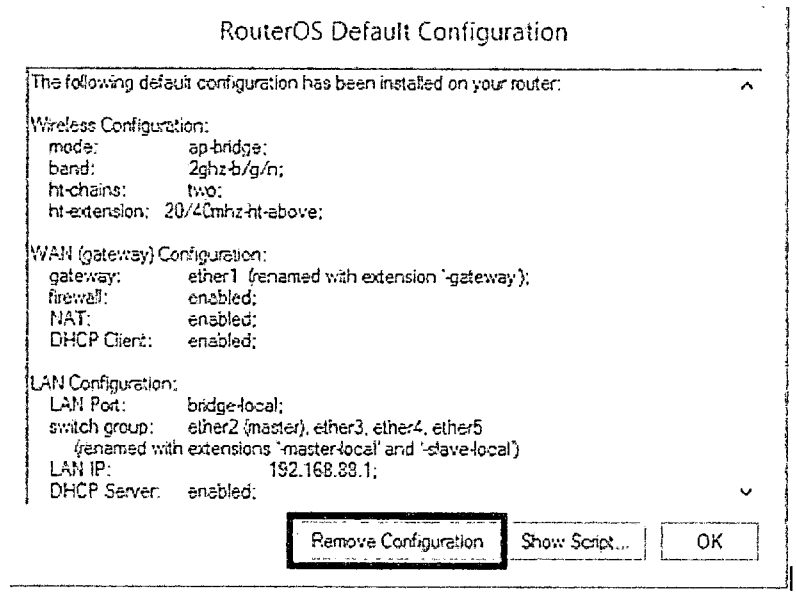


Ilustración 25 Ventana de Configuración por Defecto del Router

d. Luego hacemos clic en el botón **Interface**, esto nos mostrara una ventana en la cual se visualiza las 05 interfaces Giga Ethernet que presenta nuestro router, nosotros solo trabajamos con las interfaces ether01 y ether02 a las cuales les ingresamos una descripción haciendo doble clic en ellas.

Ether01: Conexión a Internet

Ether02: Conexión a la Red

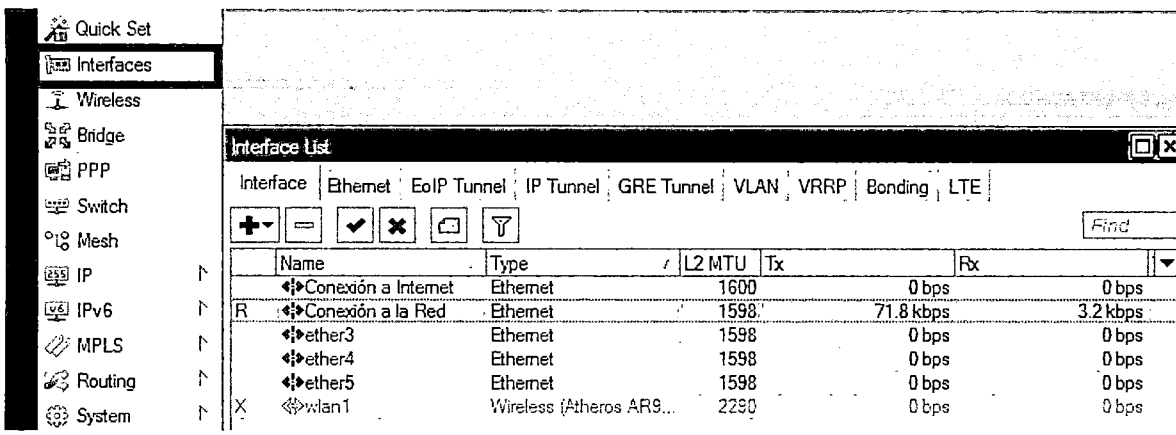


Ilustración 26 Interfaces del Router

e. Luego Ingresamos a **IP ->Addresses**, en este proceso asignaremos una IP a nuestras interfaces **(Clic en +).**

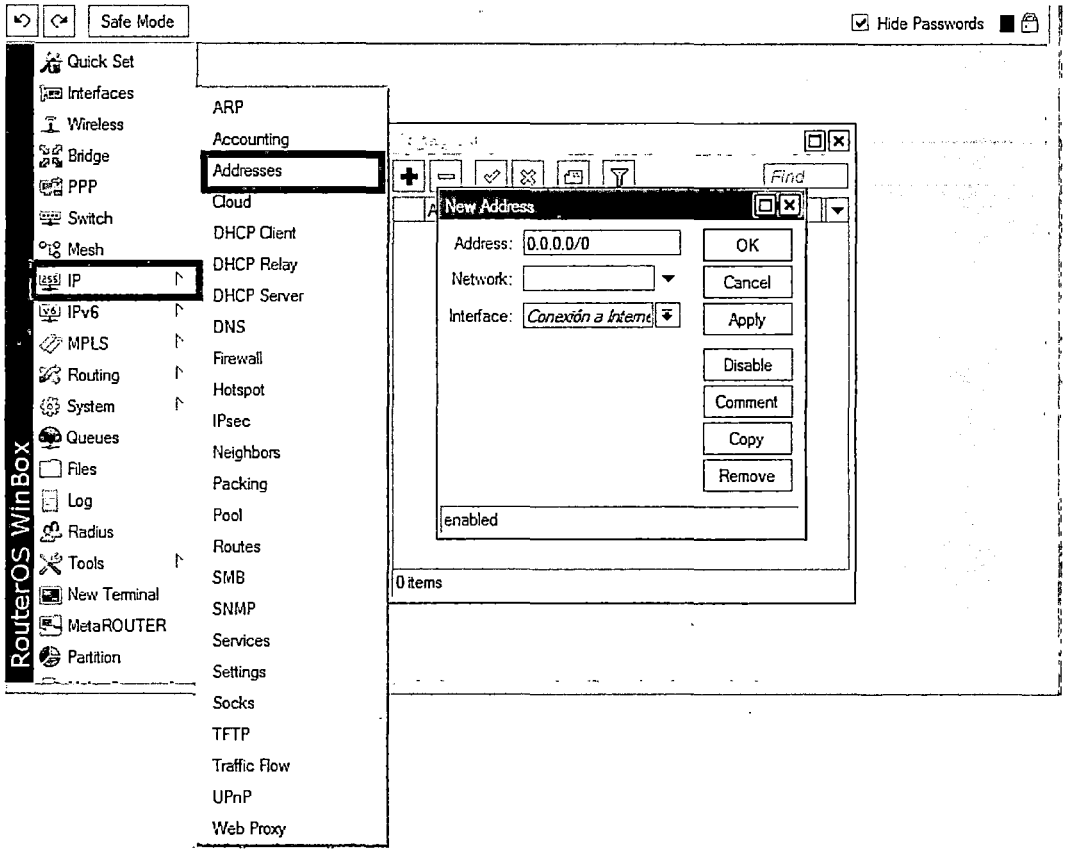


Ilustración 27 Ventana de Direcciones IP del Router

- **En address** ingresamos la IP Privada, por la cual saldremos a internet, la misma que nos fue asignada por el personal de la municipalidad con la apertura del puerto 1723. La siguiente tabla muestra las IP configuradas para cada municipalidad.

Municipalidad	IP con apertura del puerto 1723
M. Rímac	192.168.10.230
M. San Juan de Lurigancho	10.10.10.53
M. Cuzco	172.172.10.20
M. Piura	172.28.1.160
M. Castilla	192.168.1.200

Tabla 15 Dirección IP para conexión a Internet por Municipalidad

- **En Interfaces** seleccionamos ether01 (al cual le habíamos asignamos la descripción Conexión a Internet), para finalizar clic en **OK**.

- Agregamos una nueva IP, haciendo clic en **(+)**, pero en este caso asignamos una IP a ether02 (al cual le asignamos la descripción conexión a la red) esta IP fue asignada teniendo en cuenta que esté dentro del mismo segmento asignados a los operadores del centro de monitoreo, para así tener conexión con toda la red de cámaras. La siguiente tabla muestra las IP configuradas para cada municipalidad.

Municipalidad	IP de Conexion a la Red
M. Rímac	172.172.254.200
M. San Juan de Lurigancho	172.25.1.200
M. Cuzco	10.10.101.200
M. Piura	172.26.1.200
M. Castilla	172.100.21.200

Tabla 16 Dirección IP para conexión a la red interna

f. Ahora debemos asignar el Gateway al Mikrotik, este debe ser por el cual saldremos a internet ya que sin esto no tendremos gestión Remota. Ingresamos **IP -> Routes -> +**, en Gateway ingresamos nuestra IP.

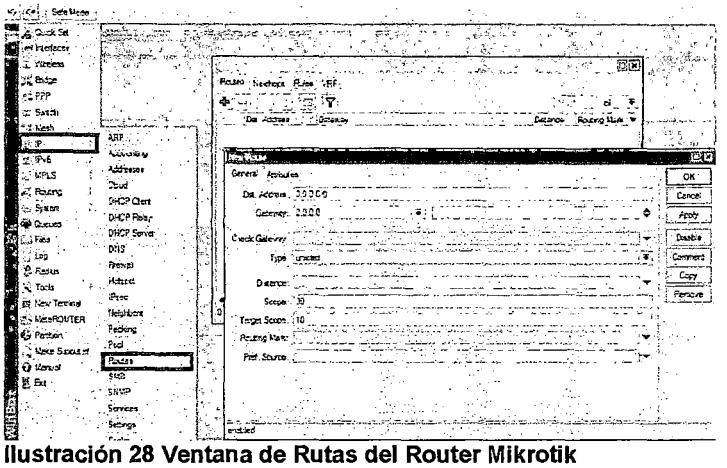


Ilustración 28 Ventana de Rutas del Router Mikrotik

La siguiente tabla muestra los gateway configurados para cada municipalidad (esto dependió del proveedor de internet), finalmente hacemos clic en **OK.**

Municipalidad	Gateway de Internet
M. Rímac	192.168.10.1
M. San Juan de Lurigancho	10.10.10.1
M. Cuzco	172.172.10.1
M. Piura	172.28.1.1
M. Castilla	192.168.1.1

Tabla 17 Gateway de Internet

g. Ingresamos a la opción **IP -> DNS:**

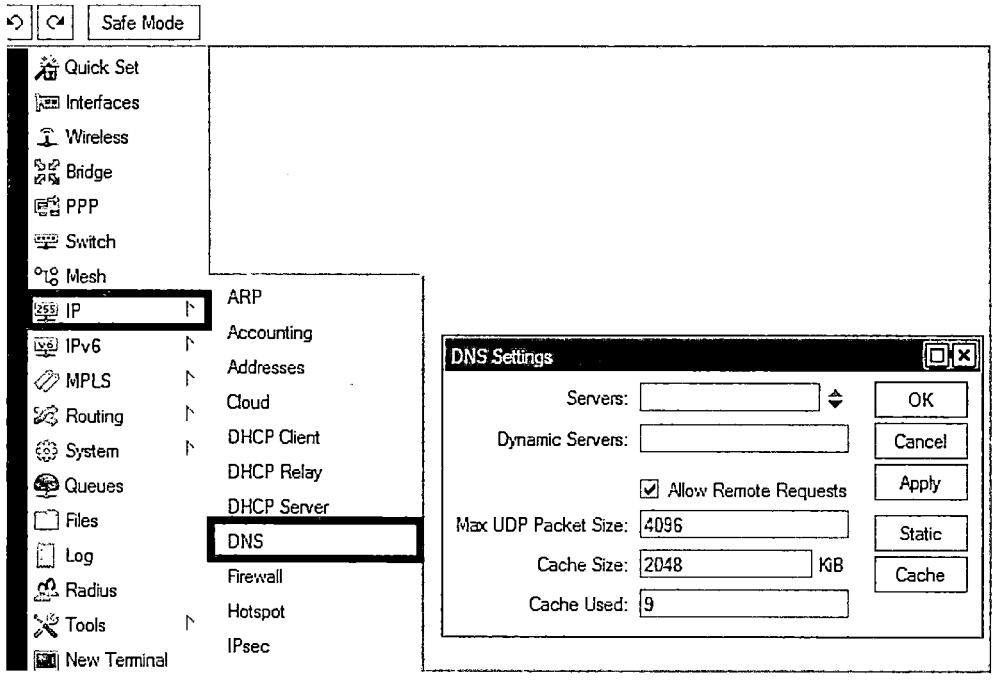


Ilustración 29 Ventana de DNS del Router Mikrotik

- **Servers:** Ingresamos los DNS asignados por el proveedor de internet
- **Activamos** la opción **Allow Remote** Request con un check.
- Finalmente clic en **OK** para guardar los cambios.

h. Ya que cada cámara con sus respectivos radios tienen asignado un segmento de red distinto, configuramos rutas estáticas para cada una, para lo cual usamos las Tablas de Direccionamiento descritas en el capítulo 3 de este documento. Para ello ingresamos en **IP -> Routes -> +:**

- En **Dst. Address:** Ingresamos el segmento de IP de cada una de las cámaras.
- En **Gateway:** Ingresamos los Gateway para conexión a la red.

Repetimos este paso para todas las direcciones IP de las cámaras, recordando que el Gateway es el mismo para todas las cámaras de una municipalidad. La siguiente tabla muestra los gateways configurados para cada municipalidad.

Municipalidad	Gateway de Conexión a la Red
M. Rímac	172.172.254.1
M. San Juan de Lurigancho	172.25.1.1
M. Cuzco	10.10.101.1
M. Piura	172.26.1.1
M. Castilla	172.100.21.200

Tabla 18 Gateway de Conexión a la Red Interna

i. Ya habiendo configurado nuestras interfaces y nuestras rutas estáticas hacia las cámaras y radios, continuamos con la configuración de las VPN Cliente:

- Ingresamos a la opción PPP en el mikrotik y seleccionamos la opción **Profile** y clic en **+**.

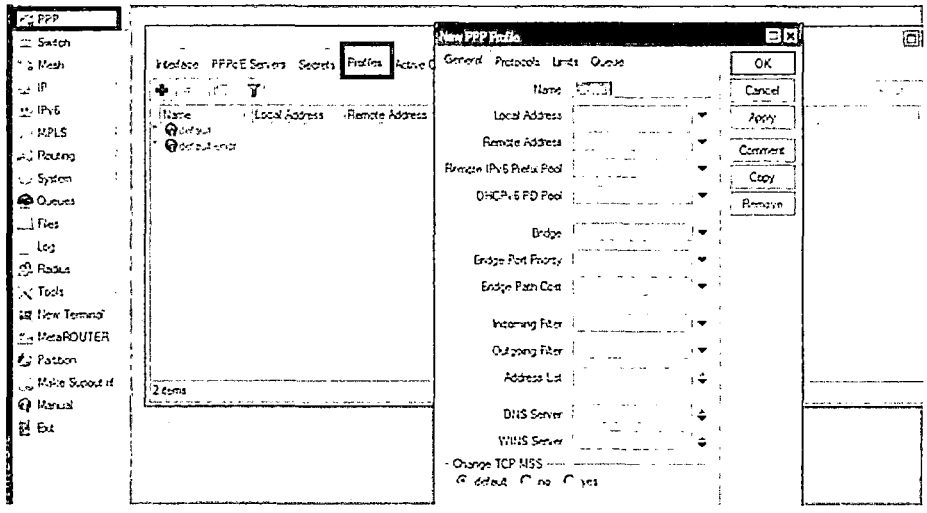


Ilustración 30 Ventana PPP del Router Mikrotik

- Fijamos el nombre del profile. En la pestaña **Protocol** en la opción **Use Encryption** seleccionamos **required**, con la finalidad de que nuestra información sea encriptado y así viaje segura a través de nuestra VPN. finalmente clic en **OK**.

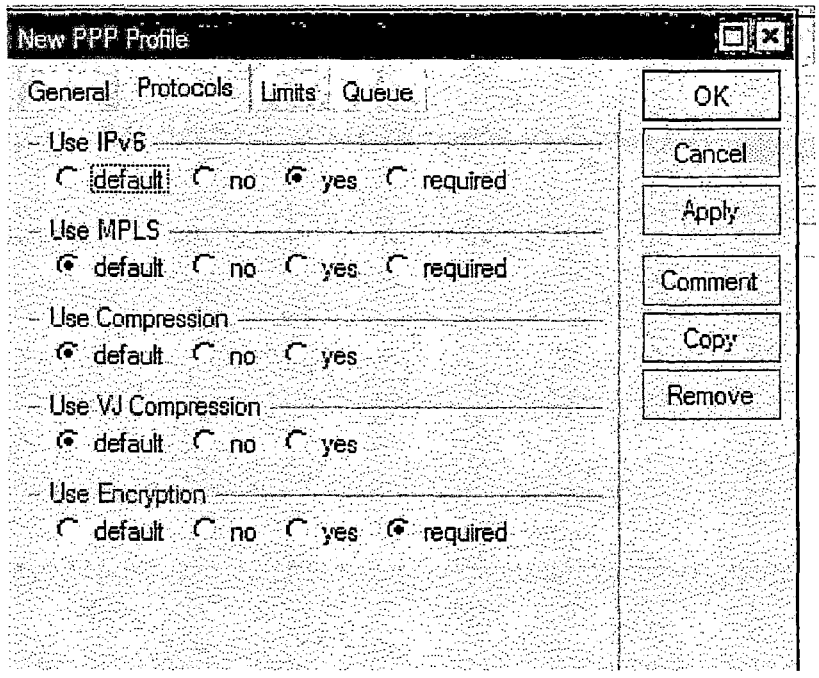


Ilustración 31 Ventana del Perfil PPP

j. Ahora crearemos los accesos a las VPN (User and password), para ello nos ubicamos en la pestaña **Secrets -> Click +:**

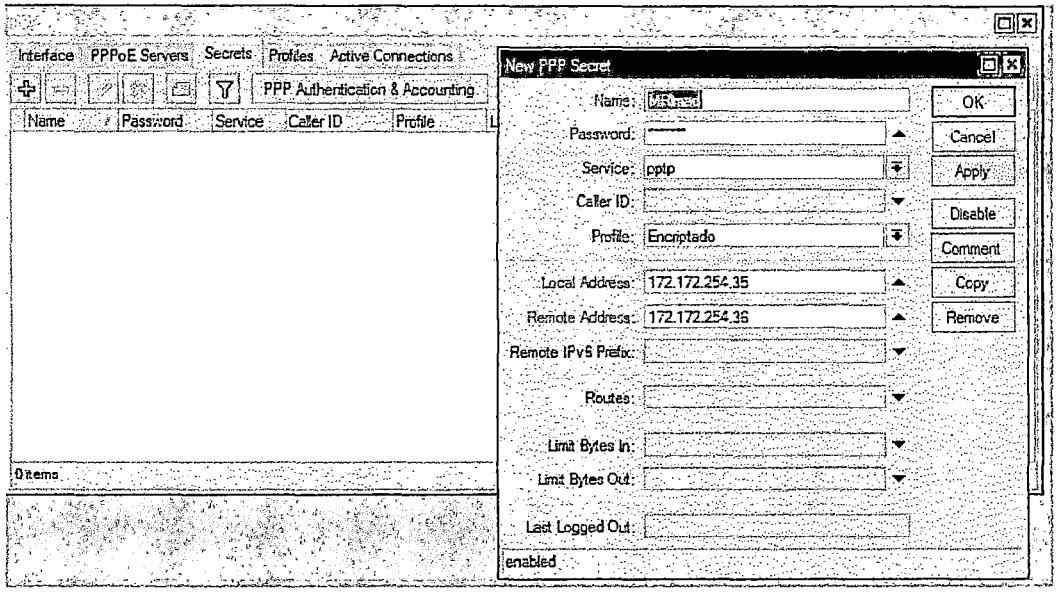


Ilustración 32 Ventana de Credenciales PPP

- **Name:** Debemos ingresar el nombre de usuario.
- **Password:** Fijamos la contraseña para el usuario ingresado anteriormente.

- **Service:** Seleccionamos PPTP, que es el protocolo para la VPN.
- **Profile:** Seleccionamos el perfil creado anteriormente (Encriptado).
- **Local Address:** Ingresamos la IP asignada a ether02 (Conexión a la Red).
- **Remote Address:** Ingresamos una IP dentro del mismo segmento de ether02(Conexión a la Red)

Clic en **OK**, para guardar los cambios

k. Ingresamos a la pestaña **interface** y seleccionamos la opción **PPTP Server**, Habilitamos el servicio en **Enable** y seleccionamos nuestro perfil creado (Encriptado) en **Default Profile,** con ello habilitamos el protocolo para la VPN, para finalizar clic en **OK.**

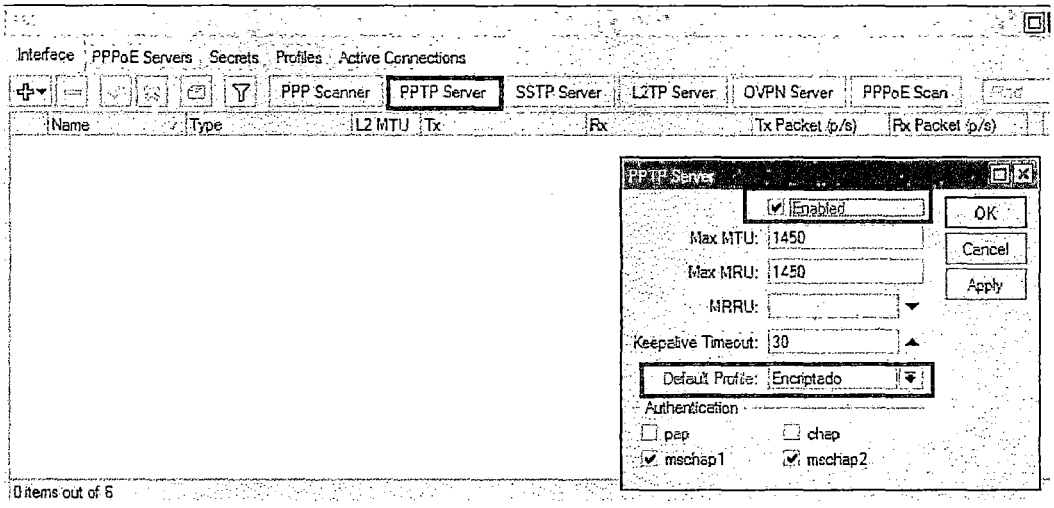


Ilustración 33 Ventana del Servidor PPTP

4.2 Implementación del VPN Servidor

En este capítulo se describe el procedimiento de la configuración paso a paso de un VPN Servidor, en el Anexo C, se muestra la configuración final del mikrotik RB1100AHx2.

Ingresamos a la configuración del Mikrotik a través de la aplicación Winbox y realizamos lo siguiente:

a. Ingresamos a la opción **IP** -> **Addresses** -> Clic **+**

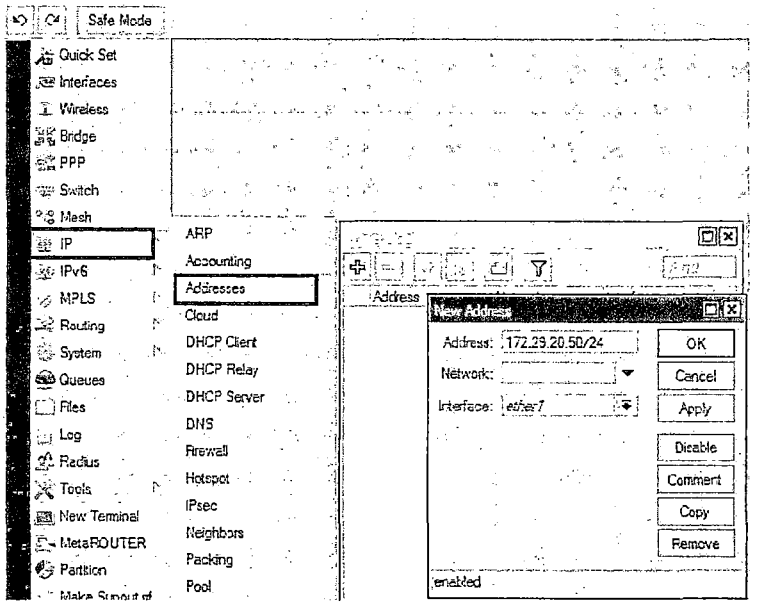


Ilustración 34 Ventana de Direcciones IP Mikrotik

- **Address:** ingresamos la IP por la cual saldremos a internet, la cual fue asignada por el personal IT de la empresa Netkrom Technologies, la cual es: **172.29.20.50/24**
- **Interface:** Ingresamos la interface de conexión entre el Router RB1100 y el Router proveedor de internet, la cual es la interface **ether01.**

b. Agregamos una nueva IP, haciendo clic en **(+)**, pero en este caso asignamos una IP a ether02 (al cual le asignamos la descripción Conexión al Servidor The Dude) esta IP es **172.200.1.1/24**

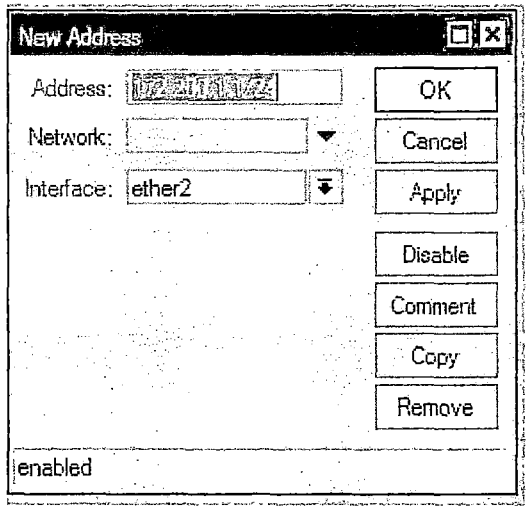


Ilustración 35 Ventana de Direcciones IP Mikrotik

c. Ahora configuramos el servidor DHCP para la interface ether02, a lo cual ingresamos a **IP -> DHCP Server -> DHCP Setup**

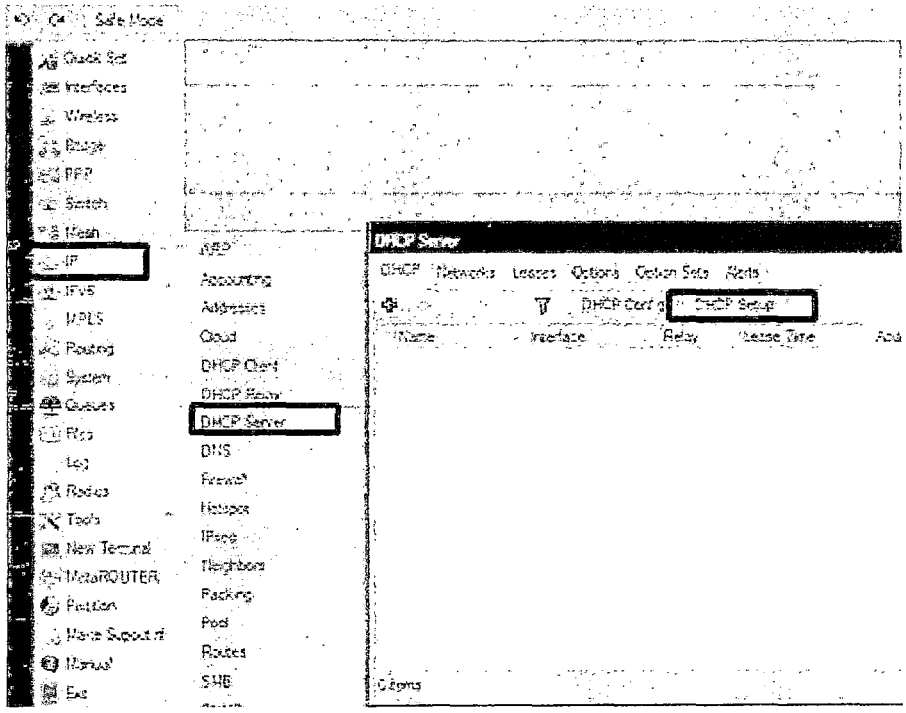


Ilustración 36 Ventana de Creación de Servidor DHCP

d. Seleccionamos la Interface **ether02** y clic en **Next** hasta recibir el mensaje de configuración exitosa.

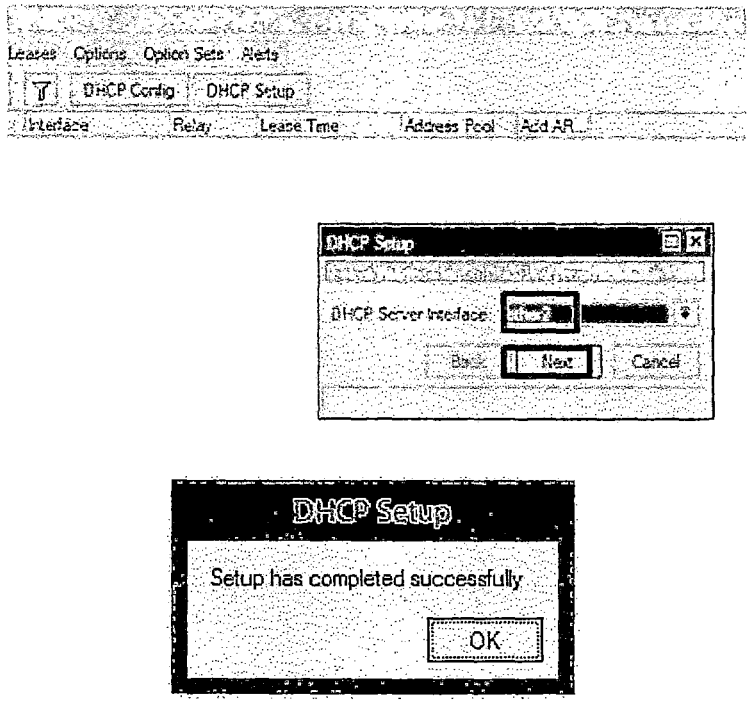


Ilustración 37 Ventana DHCP Setup

e. Ingresamos a la opción **IP -> Routes, clic en +.**

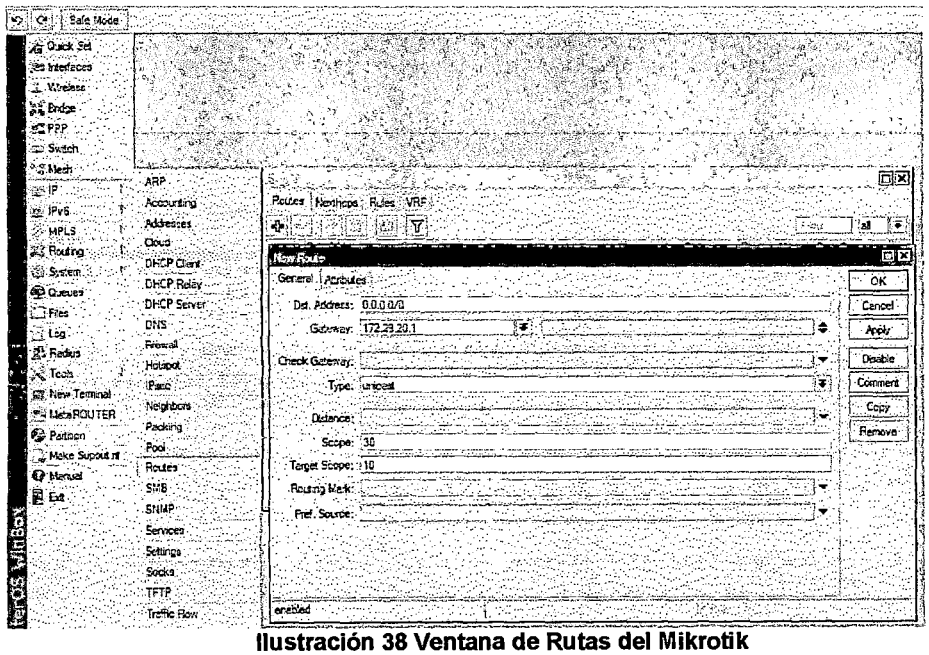


Ilustración 38 Ventana de Rutas del Mikrotik

- **Gateway**: Ingresamos la IP de la puerta de enlace del router de internet. El cual es 172.29.20.1

f. Ingresamos a la opción **IP -> DNS:**

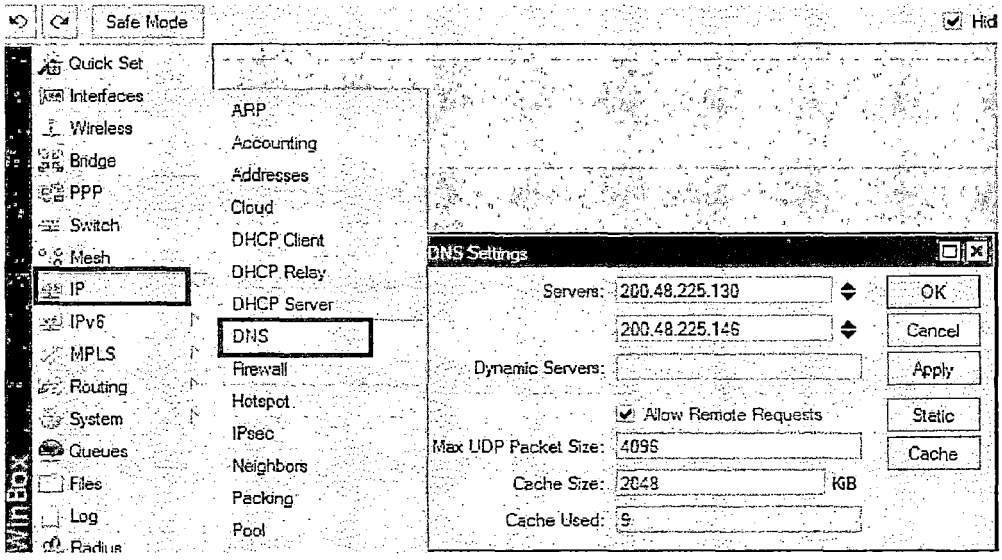


Ilustración 39 Ventana de DNS mikrotik

- **Servers:** Ingresamos los DNS asignados por el proveedor de internet, en nuestro caso fueron: **200.48.225.130** y **200.48.225.146.**
- **Activamos** un check en la opción **Allow Remote Request**.

En los siguientes pasos registraremos todas las VPN Cliente que creamos para cada municipio. ***(Estos pasos los repetimos para cada una de las VPN cliente creadas)***

g. Ingresamos a la opción **PPP,** clic en **+** y seleccionamos la opción **PPTP Client.** Ahí ingresamos la siguiente información:

- **Name:** Ingresamos el nombre de la VPN Client.

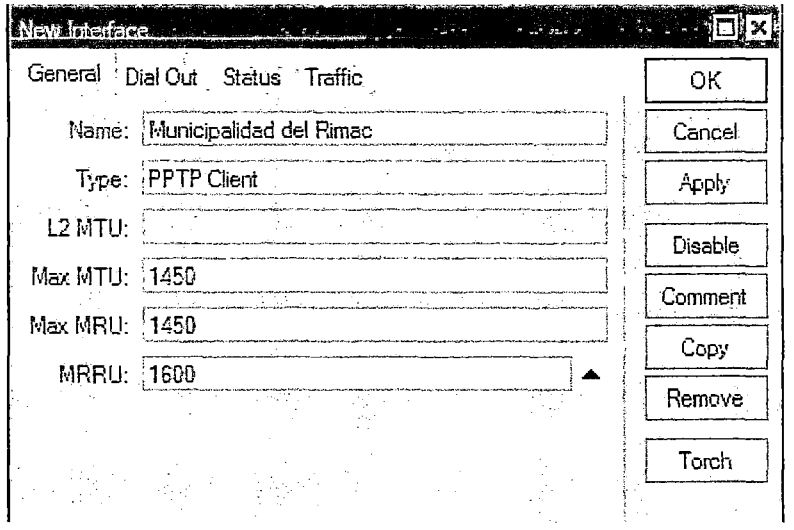


Ilustración 40 Ventana de Configuración PPTP

- Seleccionamos la pestaña **Dial Out** e ingresamos: **IP Publica** asignada por el personal de IT de cada municipalidad, el **User** y **Password** que creamos anteriormente en cada **VPN Cliente.**

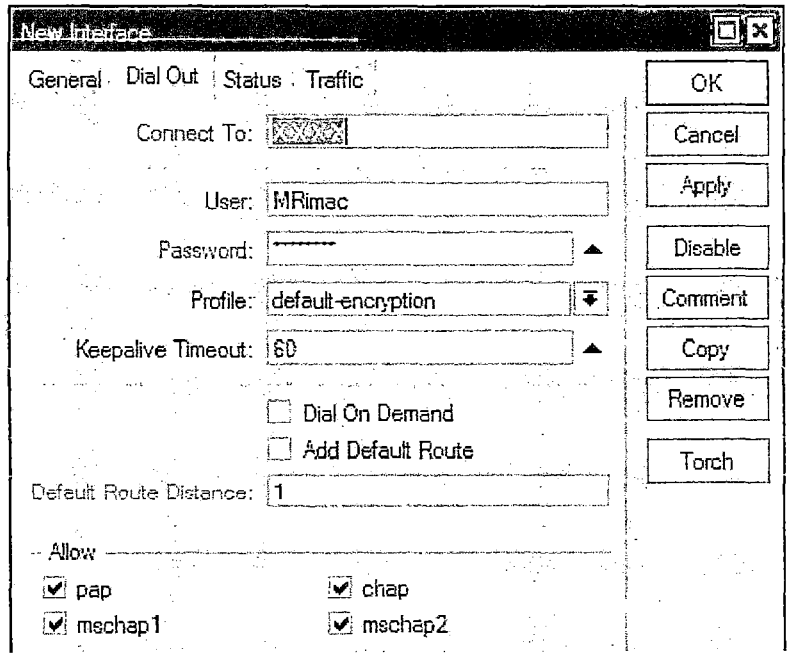


Ilustración 41 Ventana e Configuración de Credenciales PPTP

NOTA: Después de efectuada las configuraciones debe realizarse pruebas de conectividad mediante el comando PING desde cada Router Mikrotik configurado: Para realizar esto ingresamos a la opción **New Terminal** y digitamos **ping xx.xx.xx.xx.** *(Donde xx.xx.xx.xx es la ip de destino).*

CAPITULO V

DISEÑO E IMPLEMENTACION DEL SISTEMA DE GESTIÓN Y MONITOREO

CAPITULO V

DISEÑO E IMPLEMENTACION DEL SISTEMA DE GESTIÓN Y MONITOREO

5.1 Diseño del Esquemas de Gestión y Monitoreo.

Para implementar un sistema de gestión y monitoreo lo primero que se debe tener definido es lo siguiente:

- Los elementos que conforman la red.
- Los Parámetros que se van a monitorear.
- Servicios a los que se podrá acceder.
- Las alarmas que se van a configurar (definiendo el estado que llamaremos normal para cada parámetro).
- La Herramienta de gestión y monitoreo (software que realizará la acción de gestor).
- El modelo de gestión y monitoreo (protocolo que se usará para la comunicación gestor- agente).

5.1.1 Elementos de la Red: La red que se va a gestionar y monitorear es un sistema de video vigilancia por lo cual encontramos dispositivos tales como:

- Cámaras Domo PTZ VG4.
- Cámaras Domo VG5.
- Cámaras Domo 800HD.
- Radioenlace PTP AIRBR600.
- Radioenlace PTP AIRPTP600L.
- Radioenlace PTP MB-ROMBv4.
- Radioenlace PTP UBIQUITI NBM5.
- Router Mikrotik 1100AH x2.
- Router Mikrotik RB750GL

5.1.2 Parámetros: Existen muchos aspectos que se pueden monitorizar, basados en la necesidad de los administradores, para este proyecto se han elegido los siguientes:

- Conectividad de los Elementos.
- Utilización de Ancho de banda en los enlaces.
- Nivel de Señal de los enlaces.
- Consumo de CPU en los routers.
- Consumo de memoria en los routers.
- Suministro de Energía.

5.1.3 Servicios: Ya definido los elementos que se van a monitorear y teniendo en cuenta su naturaleza se configurará acceso directo a los siguientes servicios.

- Web
- Telnet
- SSH

5.1.4 Alarmas: Son consideradas eventos con comportamiento inusual. Pueden ser reportadas por un cambio de estado o basadas en parámetros con umbrales previamente configurados.

- Alarma por perdida de conectividad
- Alarma por bajo nivel de señal en un enlace (a partir de -70)
- Alarma por Alto uso de CPU (A partir del 90%)
- Alarma por Alto consumo de Memoria ((A partir del 90%)
- Alarma por corte del suministro de Energía

5.1.5 Herramientas de Monitoreo: Existen un numero extenso de software que dan solución al monitoreo y gestión de la red, pudiendo ser software libre, propietario comercial y propietario gratuito, la siguiente tabla muestra una lista con alguno de ellos.

Nombre	URL	Tipo
Argus	http://argus.tcp4me.com/	Software Libre
Cacti	http://www.cacti.net/	
freeNATS	http://www.purplepixie.org/freenats/	
Nagios	http://www.nagios.org/	
Zenoss	http://www.zenoss.com/	
OpManager	http://www.manageengine.com/products/opmanager/	Software Propietario Comercial
NetCrunch	http://www.adremsoft.com/netcrunch/	
WhatsUpGold	http://www.whatsupgold.com/	
The dude	http://www.mikrotik.com/thedude	Software Propietario gratuito

Tabla 19 Lista de Software de Gestión y Monitoreo44

Basándonos en las características técnicas de la plataforma detalladas en la siguiente tabla, y también evaluando sus ventajas y desventajas y principalmente tomando en cuenta que los administradores están familiarizados con el uso de equipamiento Mikrotik. Se decidió optar por el software **The dude.**

Especificaciones	Argus	Cacti	Free NATS	Nagios	Zenoss	Op Manager	Net Crunch	Whats UpGold	The dude
Interfaz Web	X	X		X	X	X	X	X	X
Alertas y notificaciones	X	X	X	X	X	X	X	X	X
Vasta información en la Red	X	X		X	X				
Flexible - Plugins			X	X	X				
Escalable y Robusto	X	X		X	X	X	X		X
Facilidad en Instalación y Configuración	X								X
Gráficas Estadísticas	X	X	X	X	X	X	X	X	X
Reportes			X	X			X	X	X
Autentificación	X			X		X	X	X	X

44 Tabla desarrollada por los autores

de usuarios									
Licencia Libre	X	X	X	X	X				X
Soporte protocolo SNMP	X	X		X	X	X	X	X	X
Usado para redes empresariales	X	X	X	X	X	X	X	X	X
Fácil de usar	X							X	X
Compatibilidad con Router Mikrotik									X

Tabla 20 Características de los Software de Gestión y Monitoreo[45]

5.1.6 Elección del Modelo de Gestión y Monitoreo:

Se decidió optar por el modelo de gestión de Internet basándonos en las características del tipo de red con el que contamos:

- Todos los dispositivos soportan el protocolo SNMP
- El Tráfico se envía a través del protocolo TCP/IP

5.2 Creación del Sistema de Gestión y Monitoreo.

Ya teniendo claro y detallado nuestro esquema de gestión y monitoreo iniciamos con las construcción de nuestro sistema. En el presente capítulo se detallará paso a paso la construcción del sistema de gestión y monitoreo.

5.2.1 Habilitación del Protocolo SNMP en los Dispositivos

Puesto que elegimos el modelo de gestión de internet y este trabaja con el protocolo SNMP es necesario habilitar dicho protocolo en todos los elementos de la red tales como:

- Cámaras Domo PTZ VG4.
- Cámaras Domo VG5.
- Cámaras Domo 800HD.
- Radioenlace PTP AIRBR600.

45 Tabla desarrollada por los autores

- Radioenlace PTP AIRPTP600L.
- Radioenlace PTP MB-ROMBv4.
- Radioenlace PTP UBIQUITI NBM5.
- Router Mikrotik 1100AH x2.
- Router Mikrotik 750

Para que estos elementos estén listos para las peticiones del gestor, en el Anexo D se muestra la habilitación del protocolo en los diferentes elementos de la red.

5.2.2 Instalación del Software The Dude

El monitor de red "The Dude" es una nueva aplicación de Mikrotik que puede mejorar drásticamente la forma de gestionar nuestro entorno de red. Explora automáticamente todos los dispositivos dentro de las subredes especificadas, dibuja y diseña los mapas de nuestras redes, controla los servicios de nuestros dispositivos y nos avisa en caso de que algún servicio tenga problemas.[46]

a. Descargamos el software the dude de la página http://www.mikrotik.com/thedude. (Descargamos la versión estable 3.6)

b. Luego procedimos a instalarlo en el servidor HP Compaq que se encuentra en el gabinete de la empresa Netkrom.

c. Iniciamos el Software The Dude, en la cual no pedirá que seleccionemos nuestro idioma, a lo cual seleccionamos Spanish.

46 http://www.mikrotik.com/thedude

5.2.3 Creación de los mapas de Red

En esta sección describiremos la creación de los mapas de red para cada municipalidad.

a. Para crear un mapa de red, damos doble clic en la opción **Network Maps**, clic en **+**:

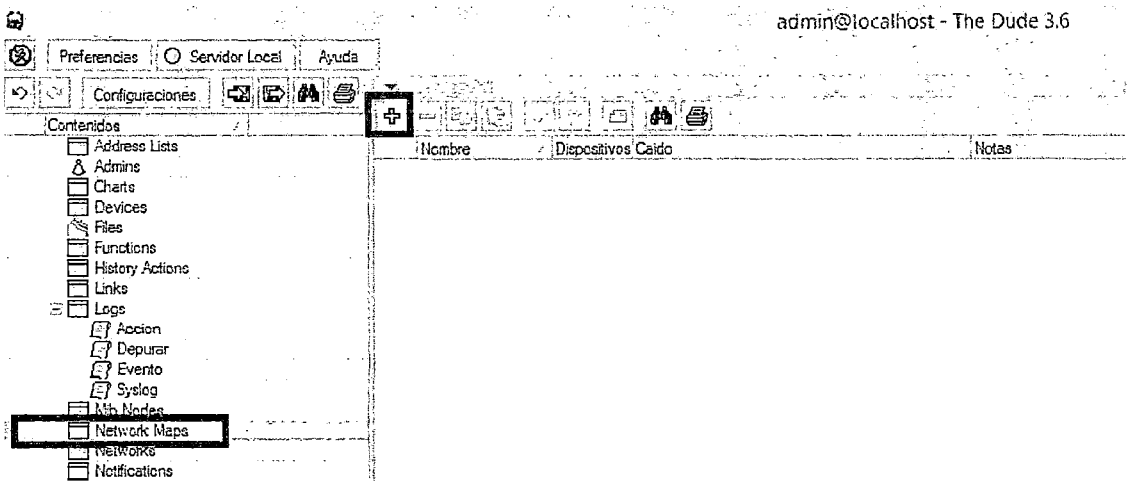


Ilustración 42 Ventana de Mapas de Red - The Dude

b. En el cuadro que aparece ingresamos el **Nombre** de nuestro mapa de red, este paso se repite para cada una de las municipalidades.

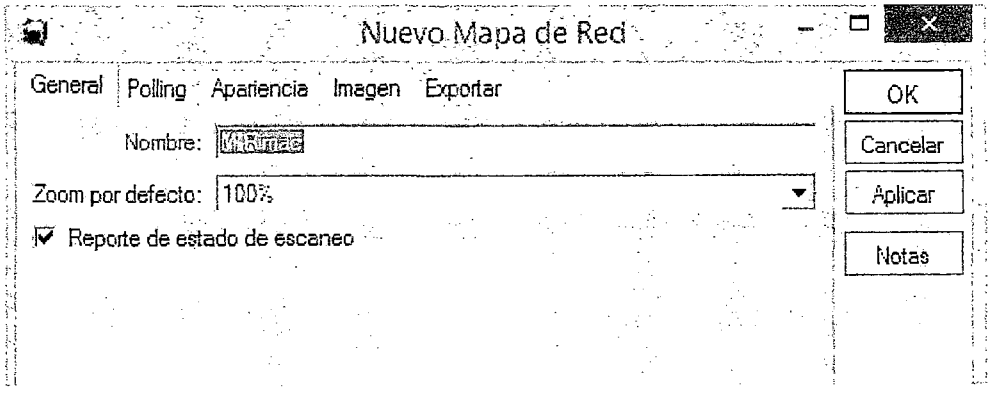


Ilustración 43 Ventana de Configuración General Mapa de Red

c. Al finalizar nos muestra todos los mapas de Red que tenemos y el número de sus dispositivos.

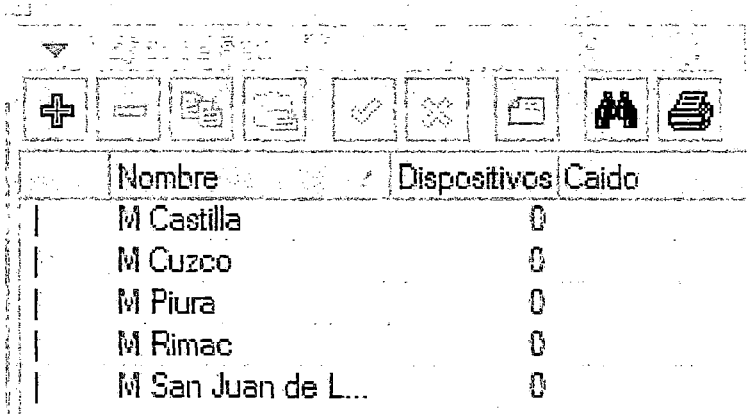


Ilustración 44 Lista de Mapas de Red

d. Luego creamos nuestros dispositivos de red, para ello hacemos doble clic en el nombre de nuestro mapa de red, y luego en **+ > Dispositivo.**

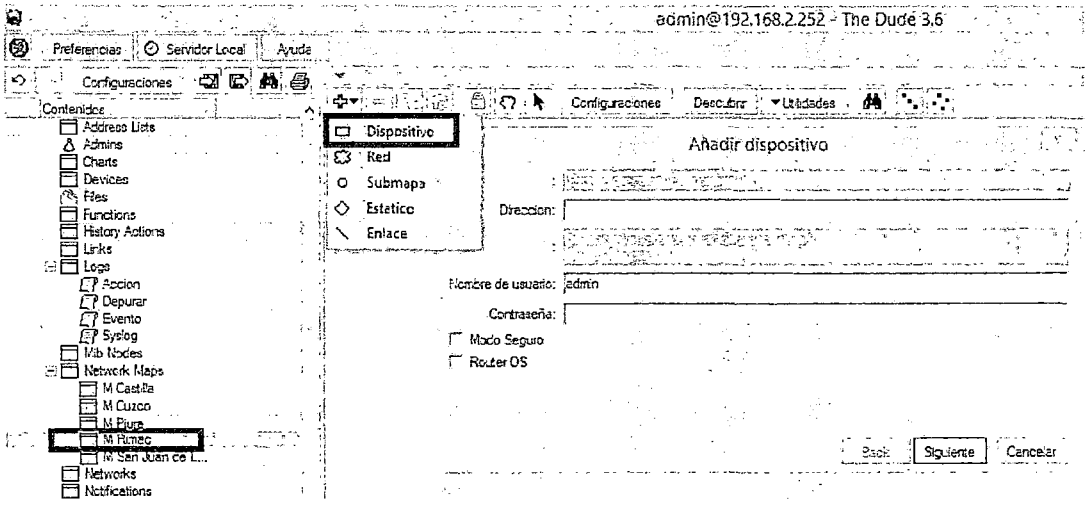


Ilustración 45 Ventana de Creación de Dispositivos

- En **Dirección** ingresamos la IP de cada dispositivo existente en la red, para este paso nos apoyamos con las tablas de direccionamiento IP descritas en el capítulo 3.
- **Nombre de Usuario** Ingresamos admin, usuario de administrador de cada equipo.

- **Contraseña** Ingresamos la contraseña para el usuario admin, y clic en siguiente.

e. Nos aparece una ventana para agregar servicios al dispositivo, clic en **+**, en la pestaña **General** configuramos pruebas de conectividad.

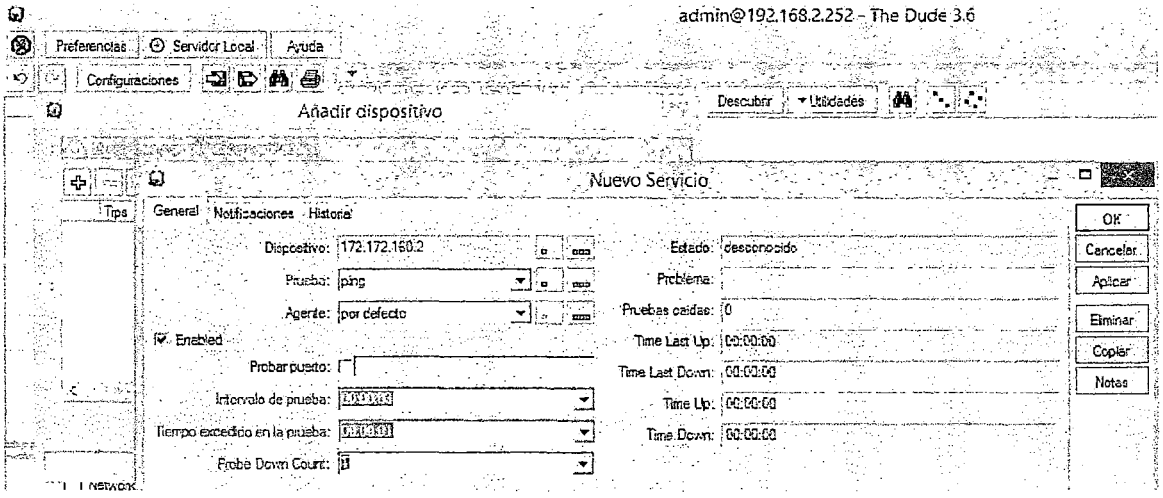


Ilustración 46 Ventana de Servicio Ping

- En **Prueba** seleccionamos ping
- **Intervalo de Prueba** Ingresamos 3 segundos
- **Tiempo Excedido en la Prueba** Ingresamos 1 segundos

Clic en Ok, y luego en Finalizar, este paso se repite para cada dispositivo.

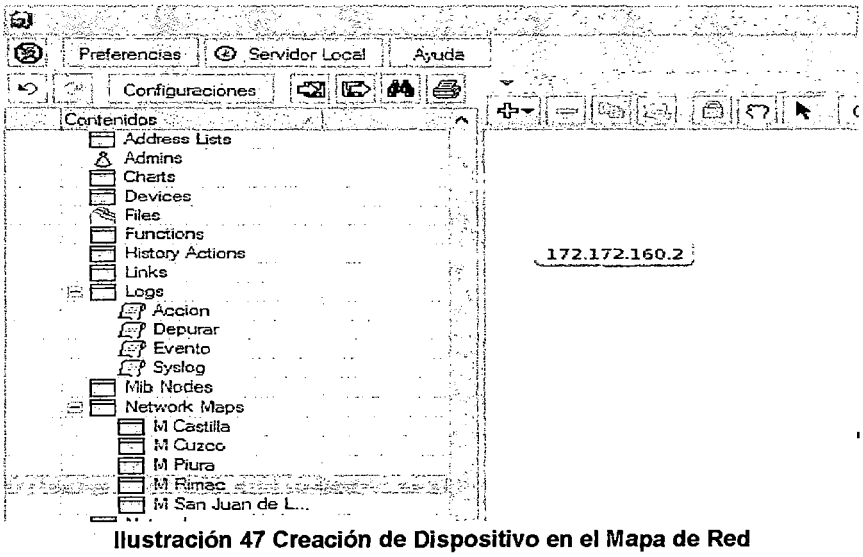


Ilustración 47 Creación de Dispositivo en el Mapa de Red

f. Ya teniendo nuestros dispositivos creados, les agregamos imagines para identificarlos. En **Apariencia > Imagen**

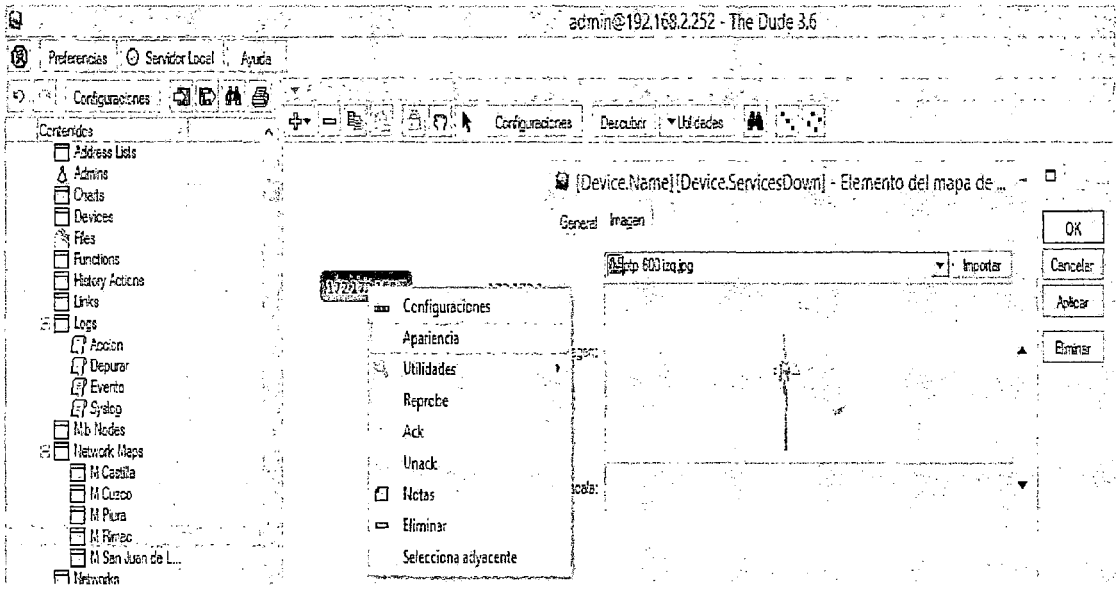


Ilustración 48 Ventana de Configuración de Apariencia de Dispositivo

g. Ya teniendo identificados los elementos creamos los enlaces, teniendo en cuenta las topologías descritas en el capítulo 3 interconectamos los elementos.

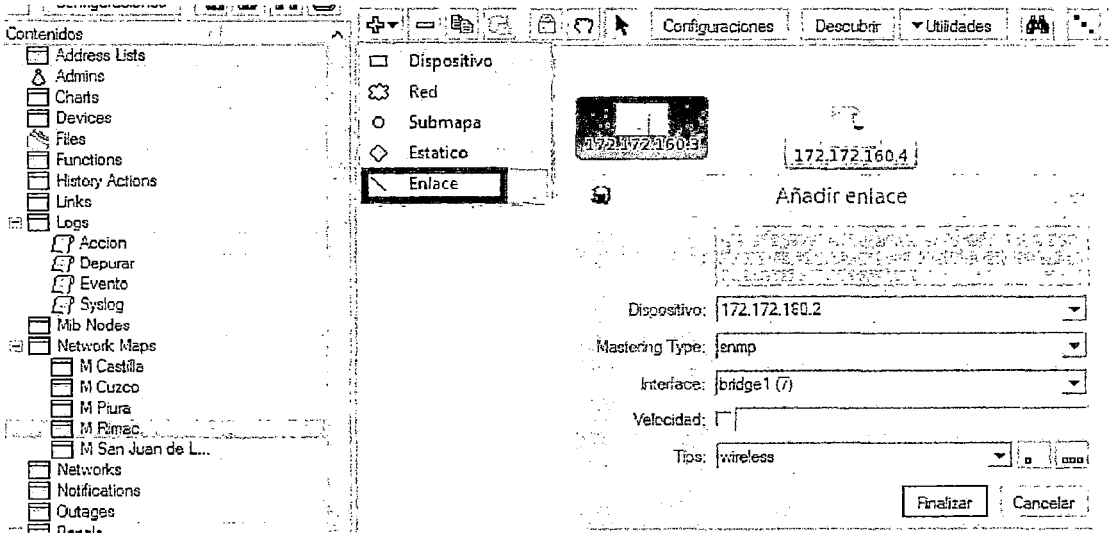


Ilustración 49 Ventana de Creación de Enlaces

- **Mastering Type:** Se selecciona SNMP, así nuestro gestor pedirá al agente los datos del throughput del enlace y los mostrará.
- **Interface:** Seleccionamos la interfaz por donde está conectado nuestro dispositivo.
- **Tipo:** Seleccionamos el tipo de conexión que tenemos, que puede ser wireless en caso de conexión aire o fast Ethernet por cable.

Y finalmente obtenemos nuestros mapas de red tal como se muestra en las siguientes figuras:

MAPA DE RED MUNICIPALIDAD RIMAC

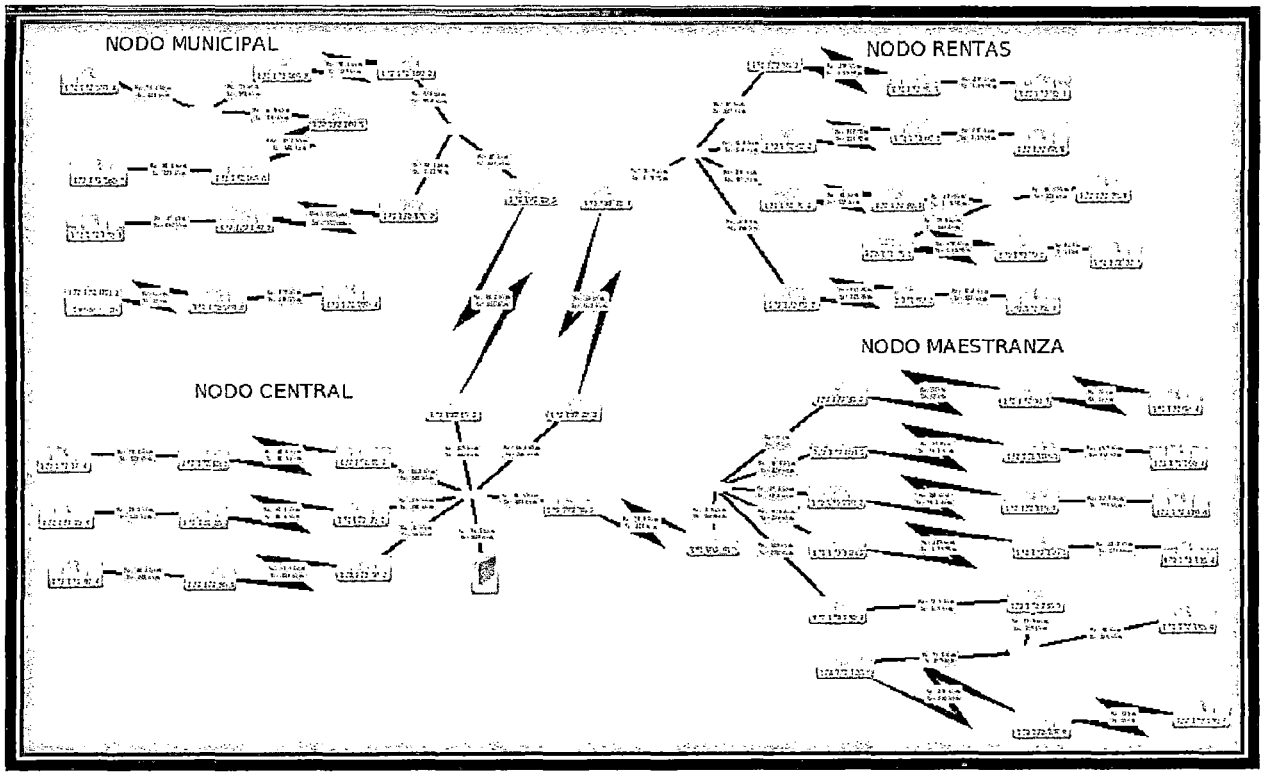


Ilustración 50 Mapa de Red Municipalidad Del Rímac - The Dude

MAPA DE RED MUNICIPALIDAD SAN JUAN DE LURIGANCHO

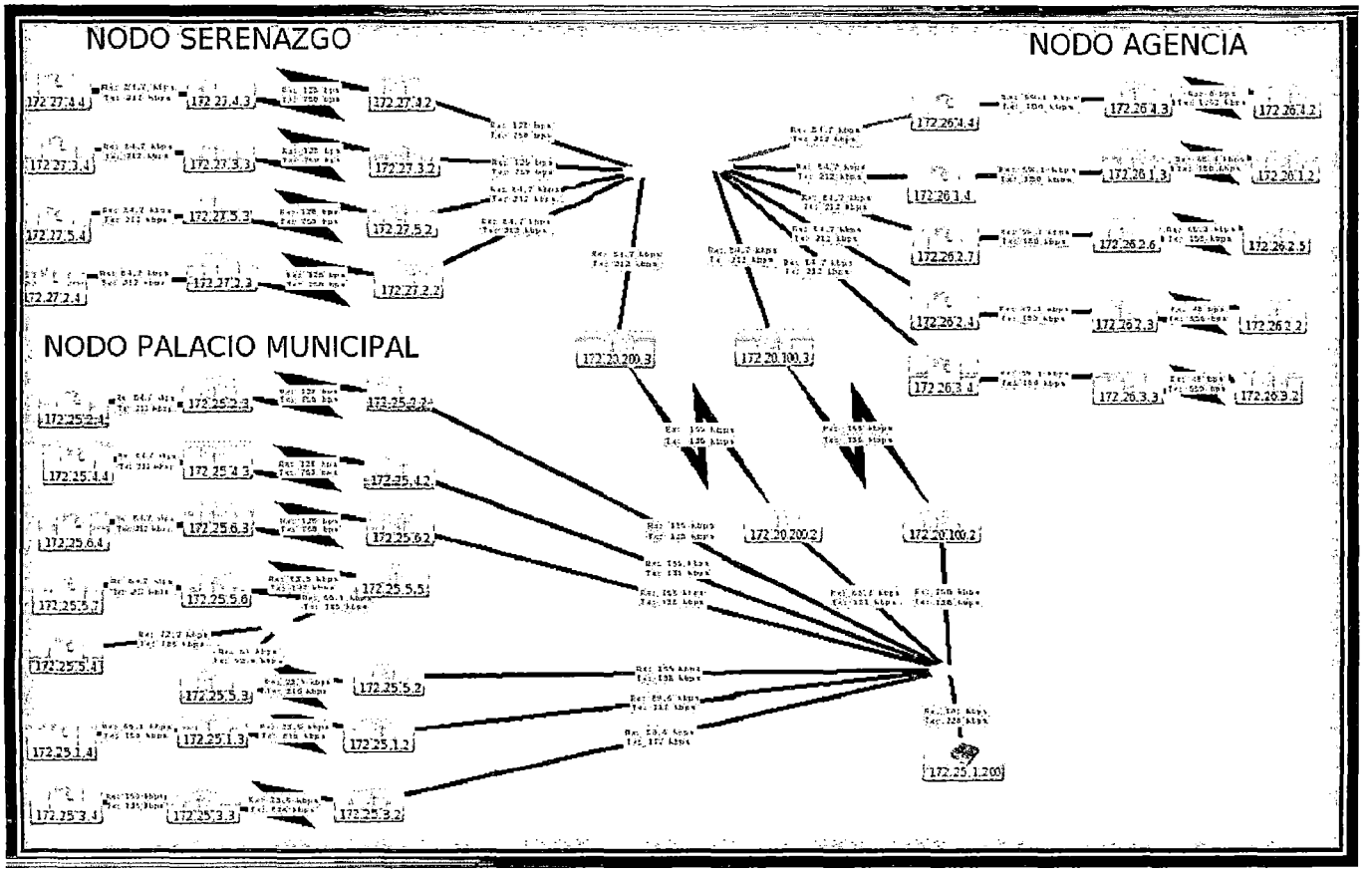


Ilustración 51 Mapa de Red Municipalidad De San Juan De Lurigancho - The Dude

MAPA DE RED MUNICIPALIDAD DEL CUSCO

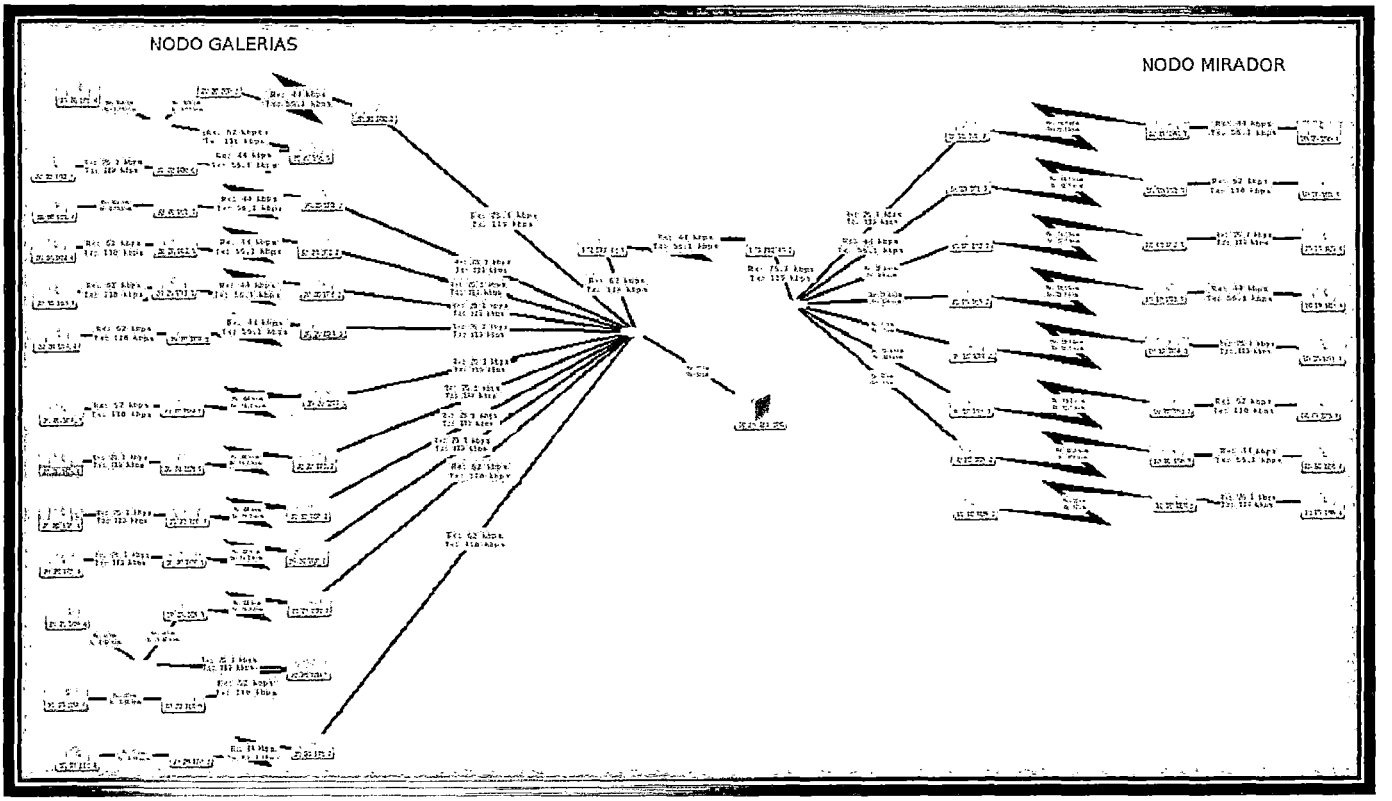


Ilustración 52 Mapa de Red Municipalidad Del Cusco - The Dude

MAPA DE RED MUNICIPALIDAD DE PIURA

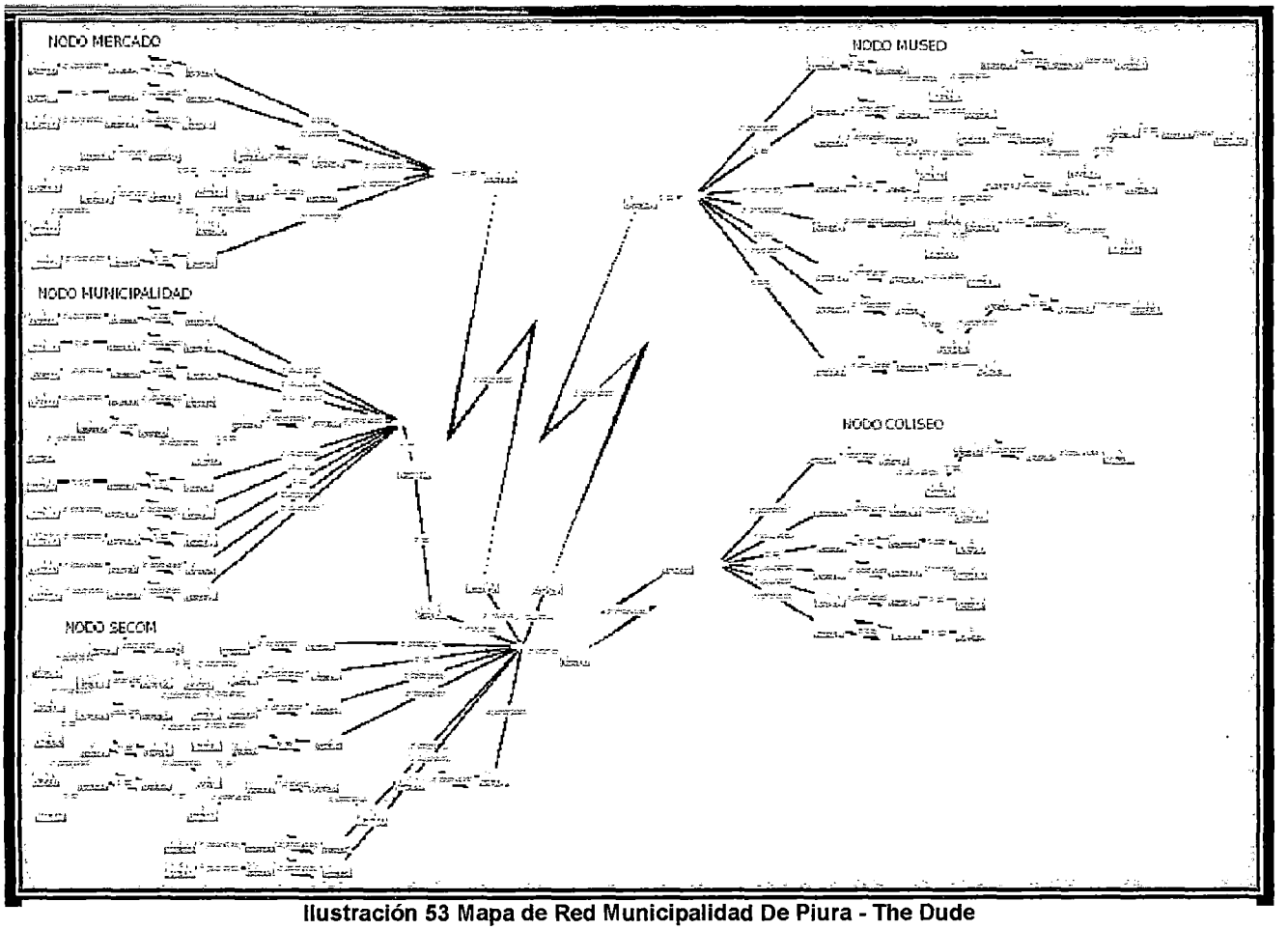


Ilustración 53 Mapa de Red Municipalidad De Piura - The Dude

MAPA DE RED MUNICIPALIDAD DE CASTILLA

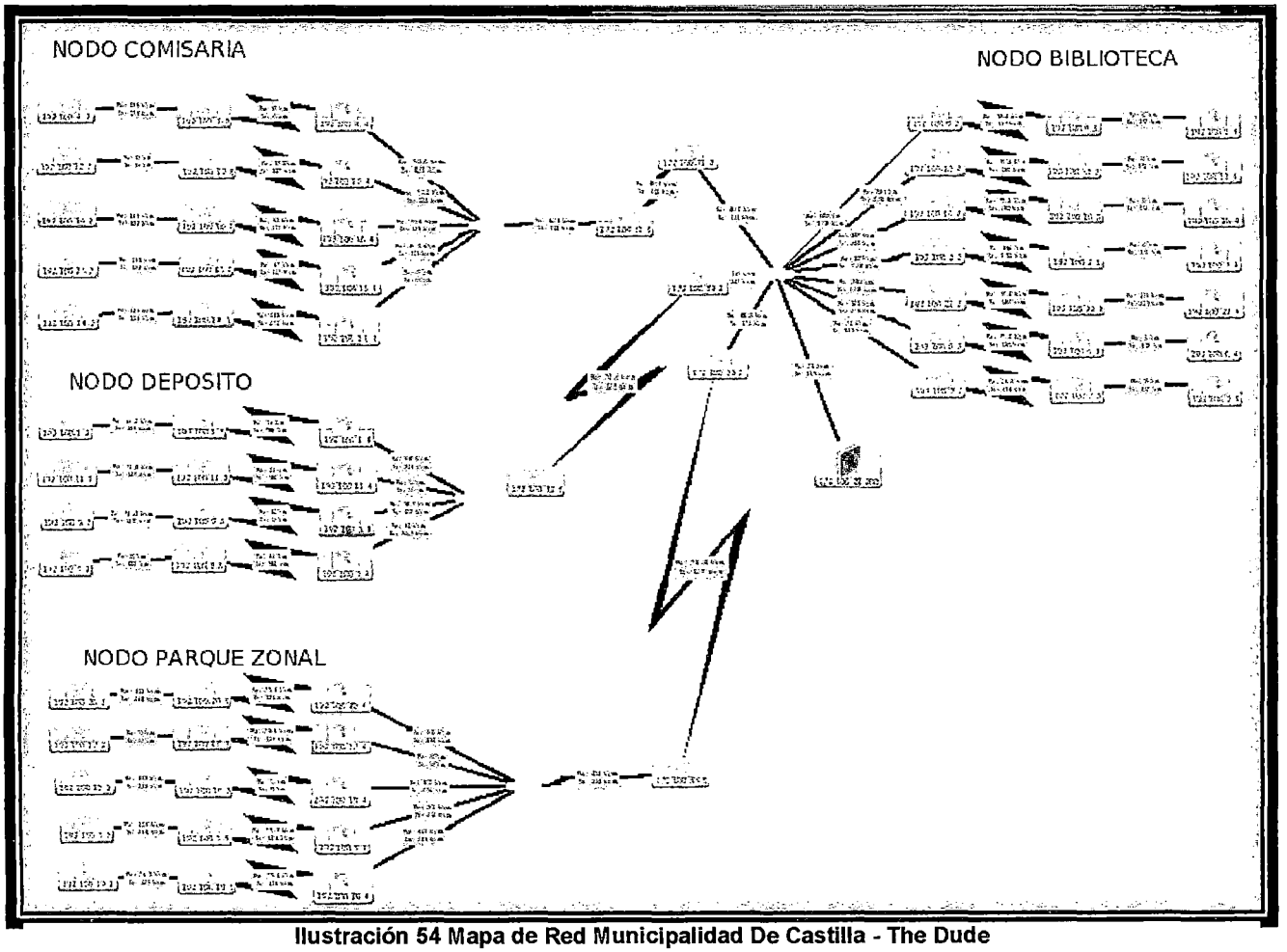


Ilustración 54 Mapa de Red Municipalidad De Castilla - The Dude

5.2.4 Configuración de los Parámetros a Monitorear

Junto con la creación de los mapas de red incluimos la configuración de dos parámetros para su monitoreo los cuales son: Conectividad de los Elementos y Utilización de Ancho de banda en los enlaces, estos fueron descritos en los pasos e y g de la sección 5.2.3 creación de los mapas de red. Por lo cual omitiremos su configuración en esta sección.

a. Configuración del Parámetro Nivel de Señal

- Para configurar el parámetro nivel de señal en los enlaces, hacer clic en **Utilidades > Indagar SNMP**

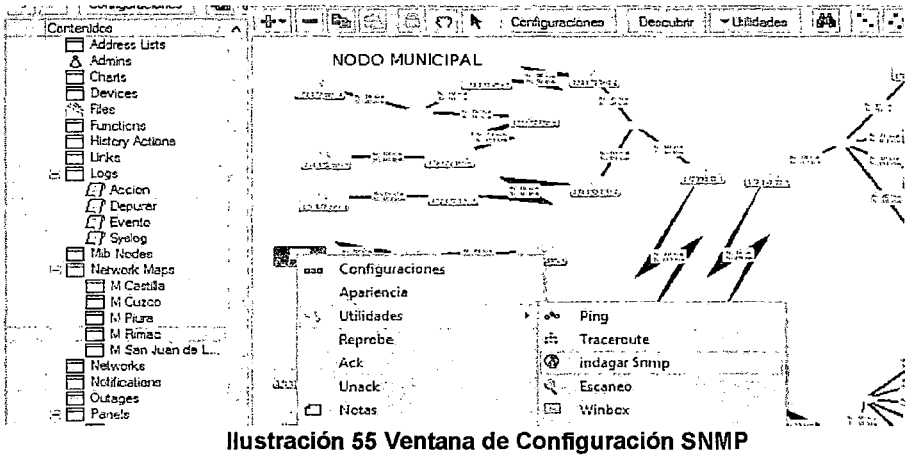


Ilustración 55 Ventana de Configuración SNMP

- Aparece un cuadro con los OID del elemento, en el cual tenemos que buscar el parámetro que deseamos monitorear para este caso el nivel de señal.

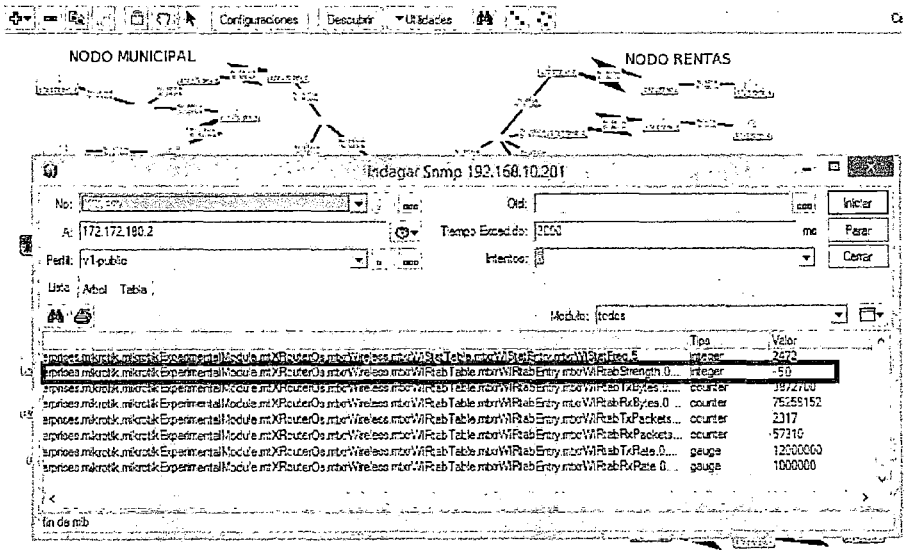


Ilustración 56 Ventana de Identificadores de Objetos OID de los Dispositivos

- Una vez identificado hacer clic en **copiar el Oid**, luego en Cerrar

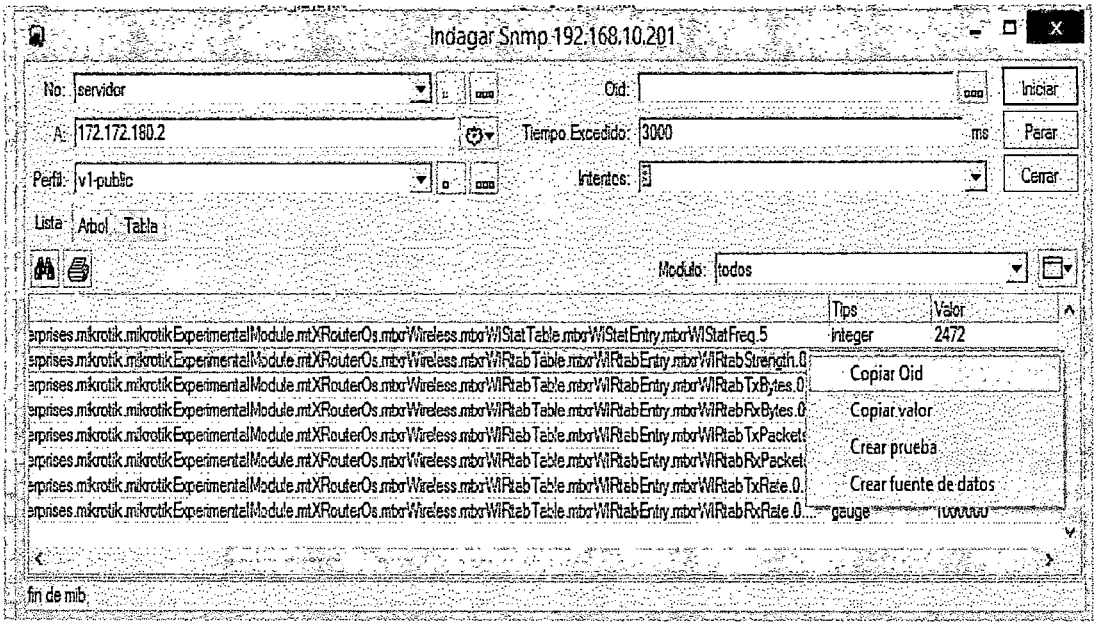


Ilustración 57 Ventana de Adquisición de OID

- En el elemento clic en **Apariencia>General**, en **Etiqueta** pegar el Oid y lo identificamos como Señal, clic en Ok

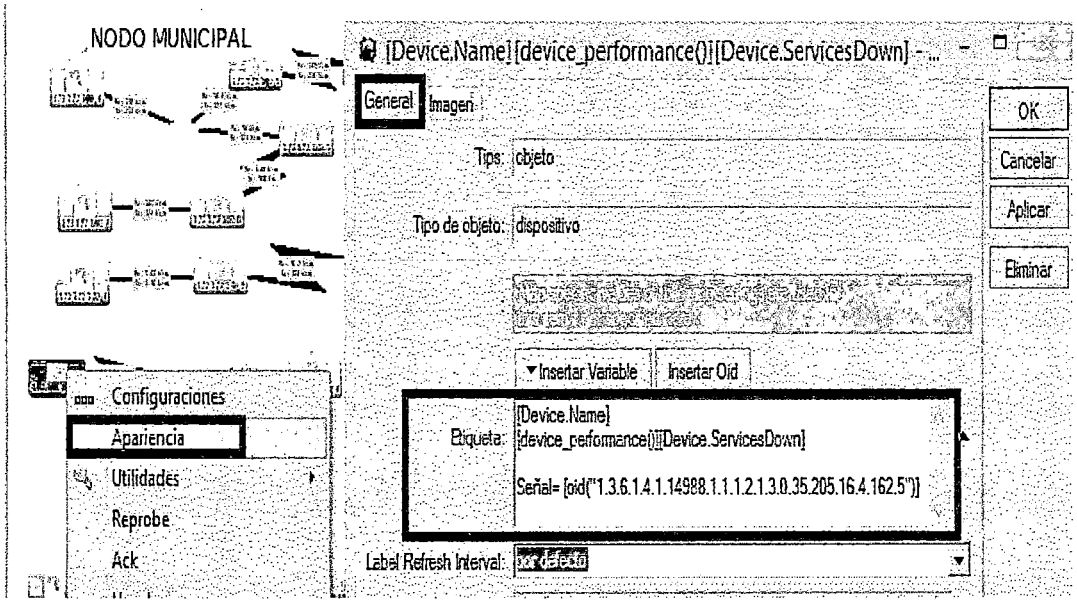


Ilustración 58 Ventana de Configuración General para Visualizar Nivel de Señal

- Finalmente podemos monitorear nuestro parámetro de nivel de señal.

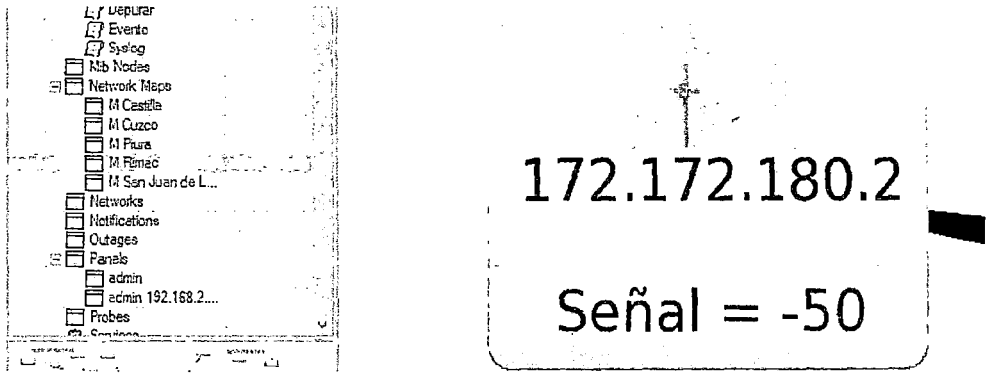


Ilustración 59 Parámetro de Nivel de Señal

b. Configuración del Parámetro Consumo de CPU y de Memoria en los routers.

- Para configurar el parámetro CPU y de Memoria en los routers, hacer clic en **Apariencia** en la pestaña **General>Etiqueta,** e ingresar el siguiente código: [device_performance()], clic en Ok

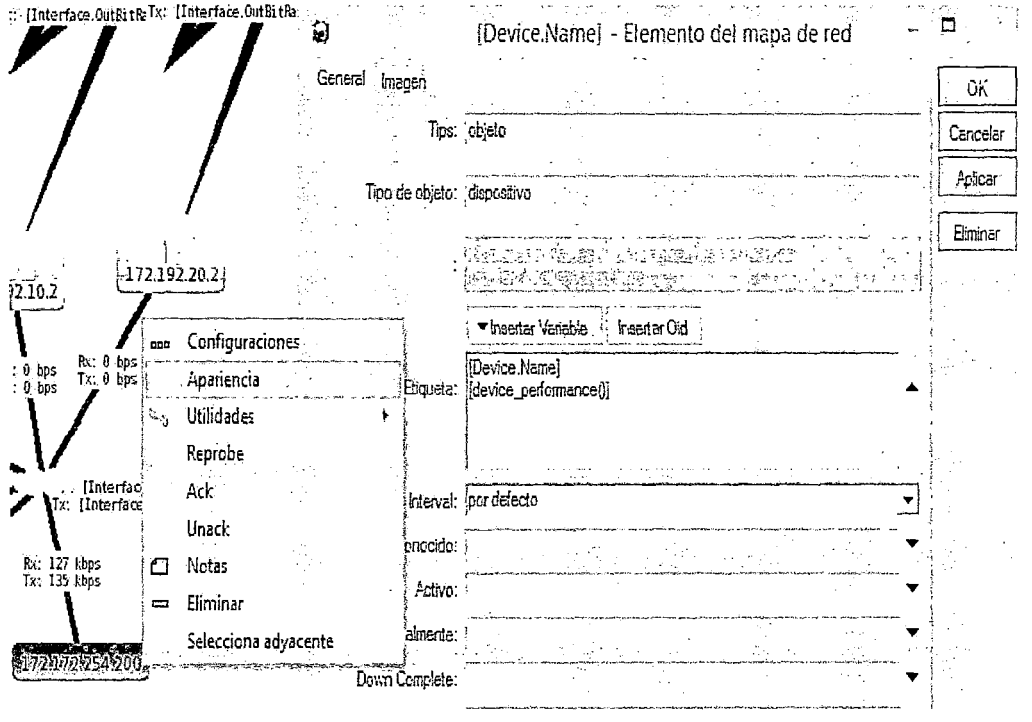


Ilustración 60 Ventana de Configuración General para Visualizar Consumo de CPU y Memoria de Routers

- Finalmente podemos monitorear nuestro parámetro.

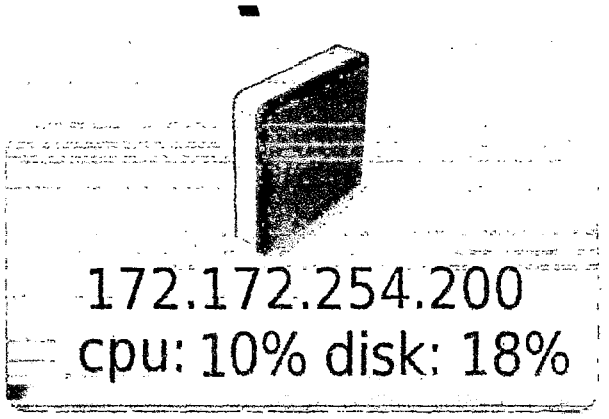


Ilustración 61 Parámetro Consumo de CPU y de Memoria en los routers

c. Configuración del Parámetro de Suministro de Energía.

- Para obtener la información de corte del suministro eléctrico, usamos las entradas de alarmas externas con las que cuentan las cámaras y los contactos secos con los que cuenta el UPS, las conexiones y configuraciones realizadas se detallan en el Anexo E.

- Para poder recibir los traps provenientes de las alarmas externas de las cámaras ingresamos a la opción **Logs>+**

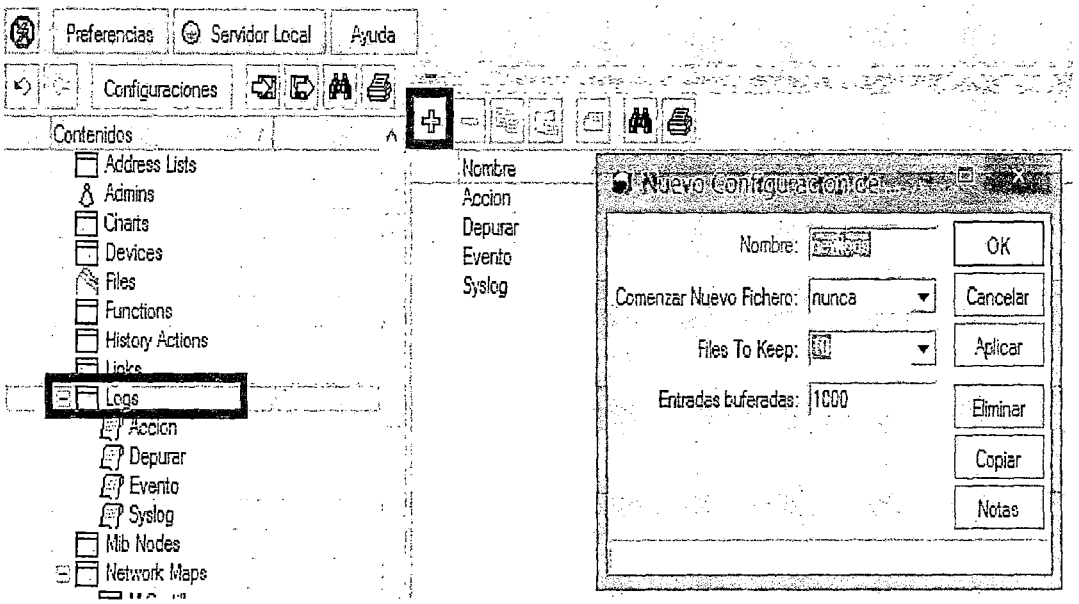


Ilustración 62 Ventana de Configuración de Logs

Llenamos los siguientes campos y clic en OK

Nombre: newlogs

Comenzar Nuevo Fichero: nunca

- Luego ingresamos a la opción **Notifications>+**, e ingresamos a la pestaña **General**

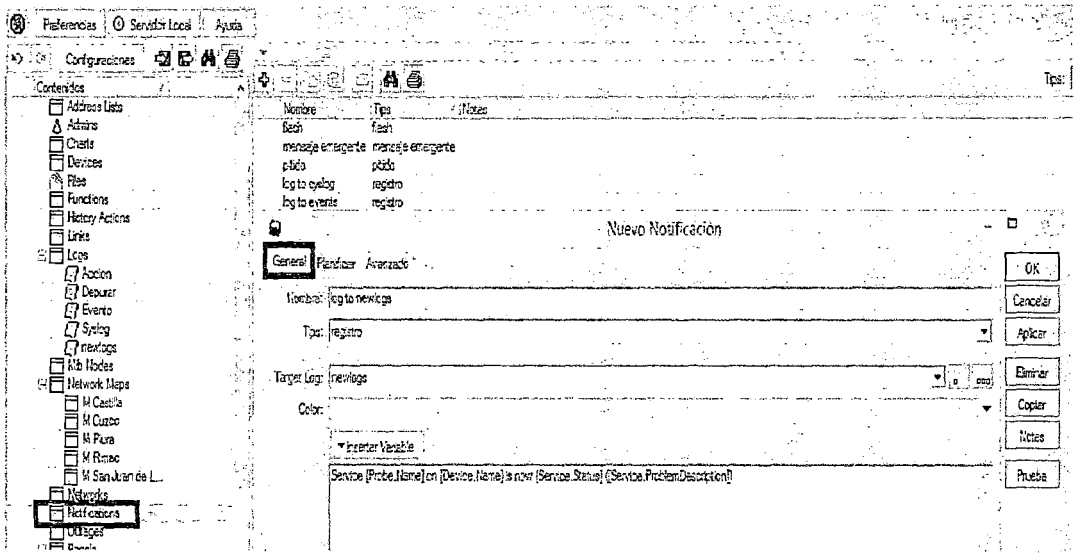


Ilustración 63 Ventana de Configuración de Notificaciones

Llenamos los siguientes campos y clic en OK

Nombre: log to newlogs

Tips: registro

Target Log: newlogs

- Luego ingresamos a la opción **Configuraciones** e ingresamos a la pestaña **Syslog**, en el ítem **Puerto** ingresamos 162, que es el puerto que se usa para los traps en el SNMP, luego clic en **+**

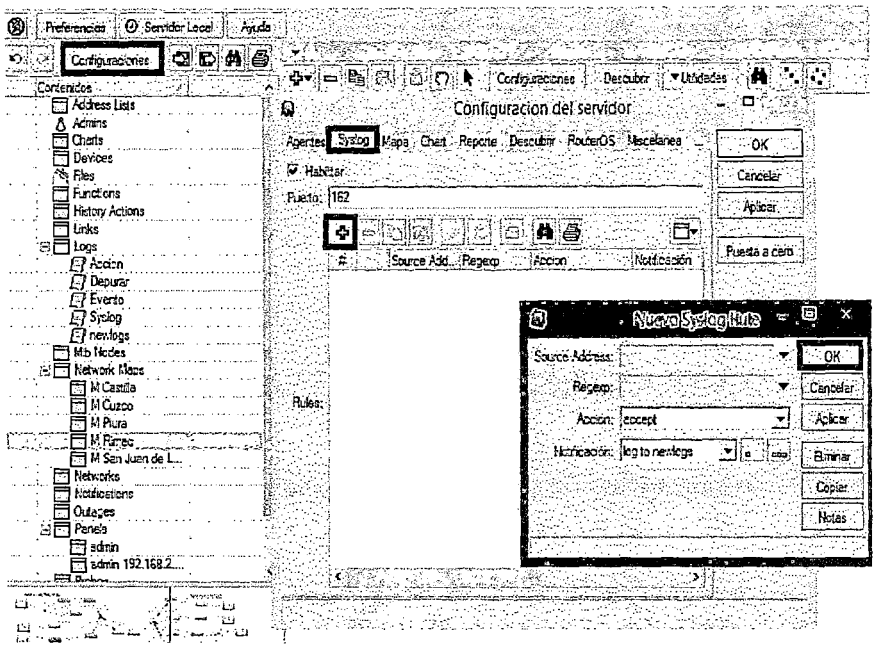


Ilustración 64 Ventana de Configuración de Traps

Llenamos los siguientes campos y clic en OK

Acción: accept, con esto aceptamos todos los mensajes que vengan dirigidos al puerto definido (162)

Notificación: log to newlogs, con ello los dirigimos hacia el registro que anteriormente creamos.

Finalmente visualizaremos los mensajes en el registro newlogs

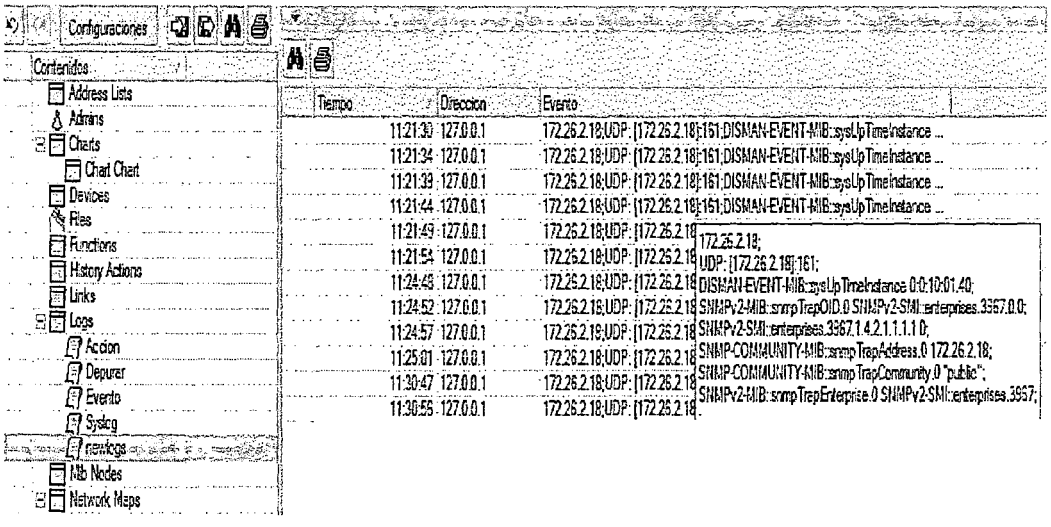


Ilustración 65 Registros de Traps Recibidos

5.2.5 Configuración de las Alarmas

Después de configurados los parámetros a monitorear creamos alarmas para informar de estados anormales en dichos parámetros.

a. Alarma por perdida de conectividad

Primero se creó una notificación con el mensaje emergente: "IP del Dispositivo fuera de servicio" para lo cual se realizó los siguientes pasos:

- En la opción **Notifications>+**, e ingresamos a la pestaña **General**

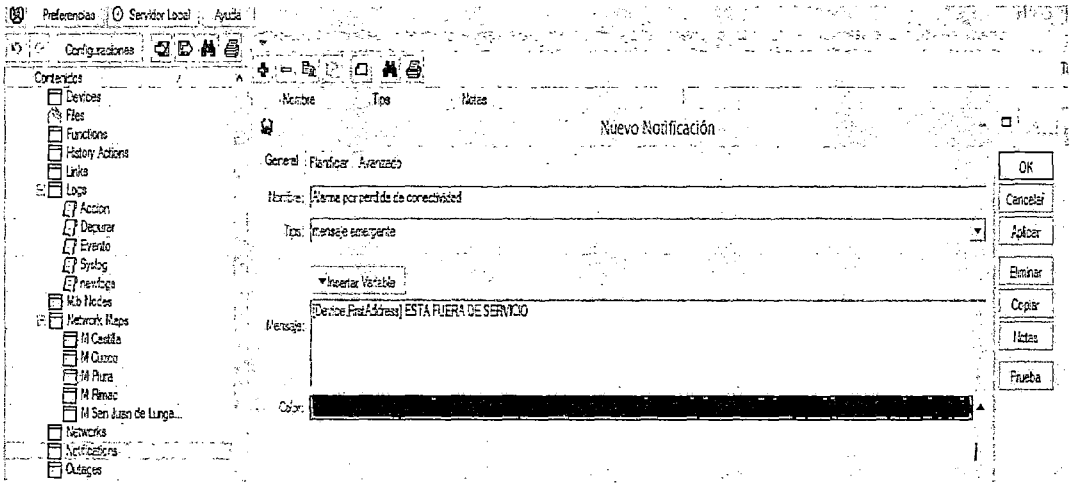


Ilustración 66 Ventana de Configuración de Notificación Para Alarma Por Pérdida de Conectividad

Llenamos los siguientes campos y clic en OK

Nombre: Alarma por perdida de conectividad

Tips: mensaje emergente

Mensaje: [Device.FirstAddress] ESTA FUERA DE SERVICIO; con ello nos mostrara la IP del dispositivo e indicaremos el problema.

Color: Seleccionamos el color rojo por ser una alarma crítica.

Ya teniendo la notificación creada vamos a asociarla al servicio de ping para ello se realizó lo siguiente:

- En la opción **Servicios** ubicamos los **Ping** y damos doble clic sobre ellos, luego vamos a la pestaña general y configuramos el tiempo de excedido de la prueba de ping en 3 segundos.

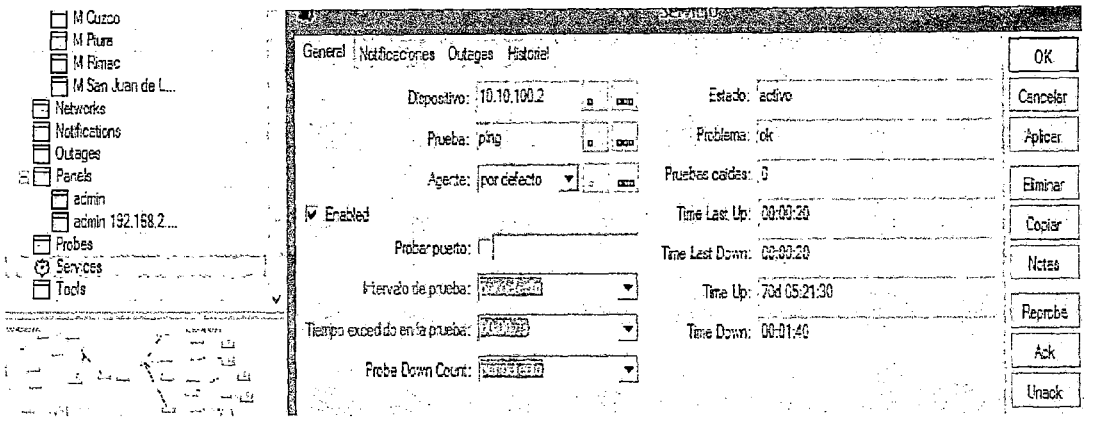


Ilustración 67 Ventana de Configuración del Servicio Ping

- Luego en la pestaña **Notificaciones,** activamos con un check en "Use Notifications", y luego seleccionamos las siguientes notificaciones:

  Alarma por pérdida de conectividad; con lo cual aparecerá el mensaje emergente creado en los pasos anteriores.

  Log to events; así tendremos el historial de las veces que los dispositivos estuvieron fuera de servicio.

  Pitido; para darle sonido a la alarma.

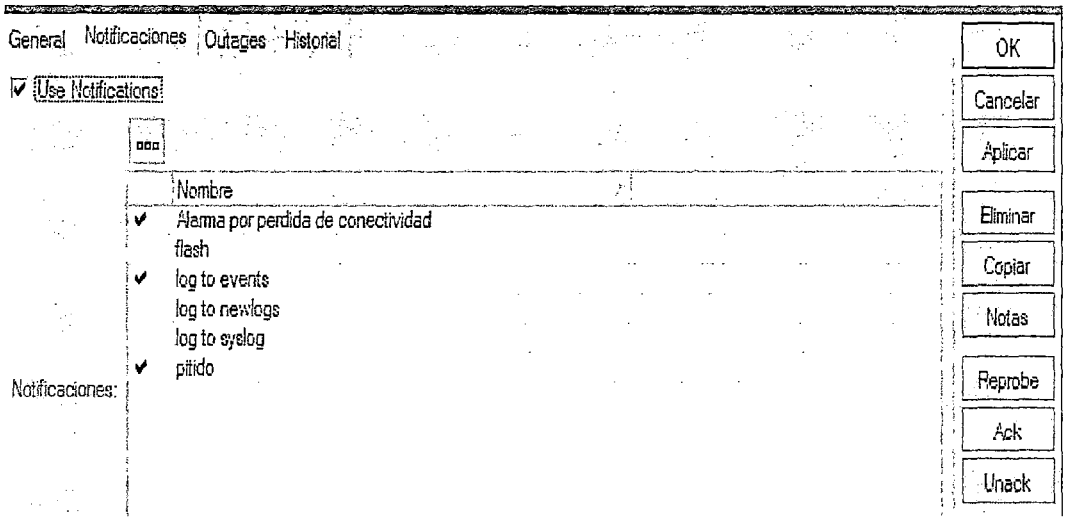


Ilustración 68 Ventana de Configuración de Notificaciones Para Alarma Por Perdida de Conectividad

El mensaje emergente se muestra de la siguiente manera:

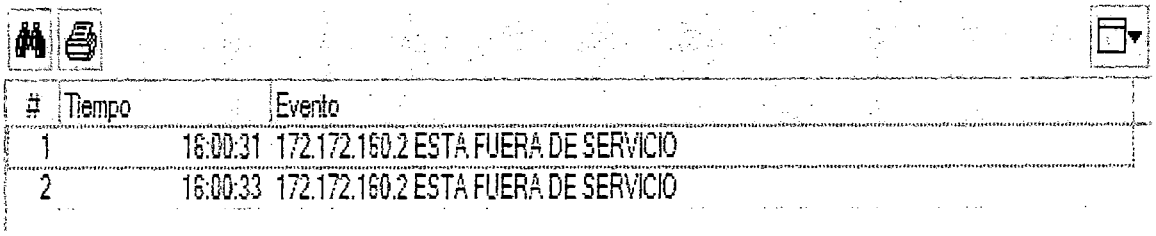


Ilustración 69 Mensaje Por Alarma de Perdida de Conectividad

También podemos ver el número de las veces que un dispositivo ha estado fuera de servicio, en que fechas ocurrieron, cuanto duro y cuál es el estado actual del evento.

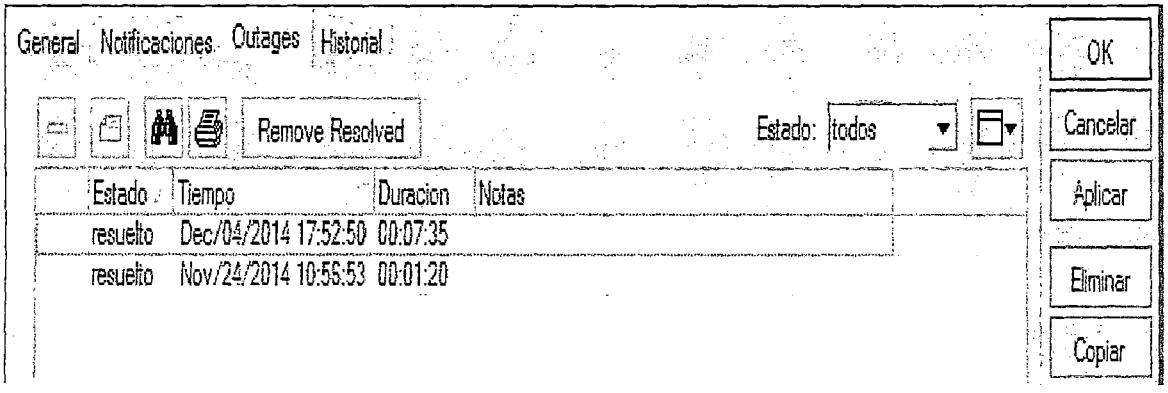


Ilustración 70 Historial de Registro de Alarma Por Perdida de Conectividad

b. Alarma por bajo nivel de señal en un enlace (a partir de -70)

Primero se creó una notificación con el mensaje emergente: "IP del dispositivo Bajo Nivel de Señal".

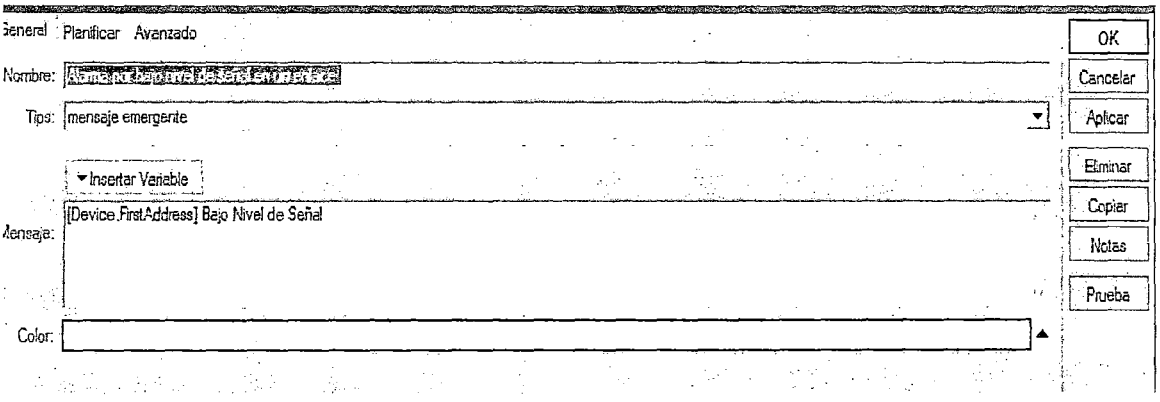


Ilustración 71 Ventana de Configuración de Notificación Para Alarma Por Bajo Nivel de Señal

Luego creamos una regla en la que indiquemos que si el nivel de señal es menor a -70 se active las notificaciones creadas para ello hicimos lo siguiente:

- En la opción **Probes>+,** Llenamos los siguientes campos y clic en OK:

  Nombre: Nivel de Señal

  Tips: SNMP, el protocolo por el cual obtenemos los datos.

  Oid: pegamos el OID correspondiente al nivel de señal.

  Tipo de Oid: Seleccionamos integer

  Método de Comparación: > (mayor) se eligió esta opción por que esta se activa cuando la regla oid>-70 es falsa.

  Valor Entero: -70,

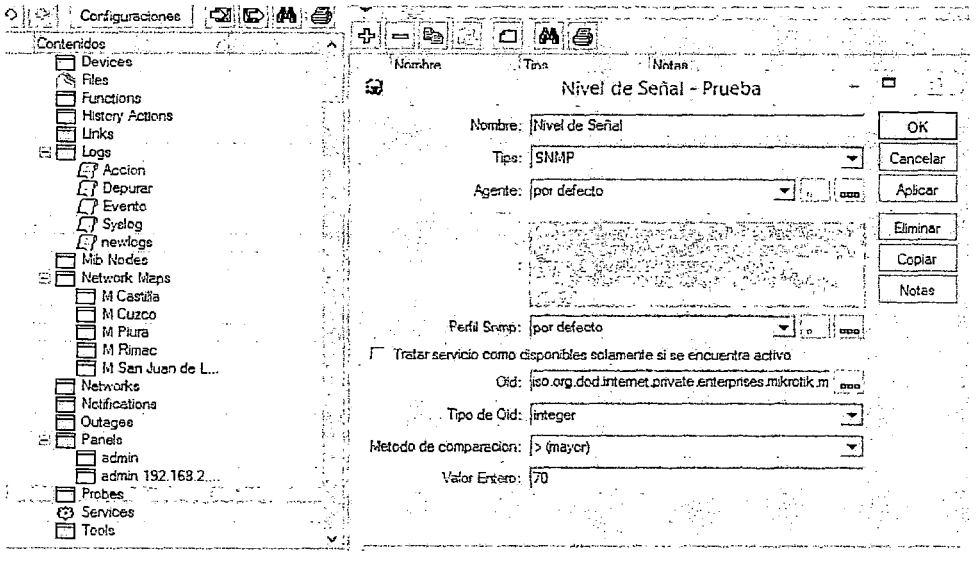


Ilustración 72 Ventana de Configuración de Niveles de Señal

Teniendo creada la regla y la notificación procedemos a activarla y asociarlas, para ello realizamos lo siguiente.

- Doble clic en los dispositivos y en la pestaña general llenamos lo siguiente

  Prueba: Nivel de Señal

  Intervalo de prueba: 3 segundos

  Tiempo excedido en la prueba: 3 segundos

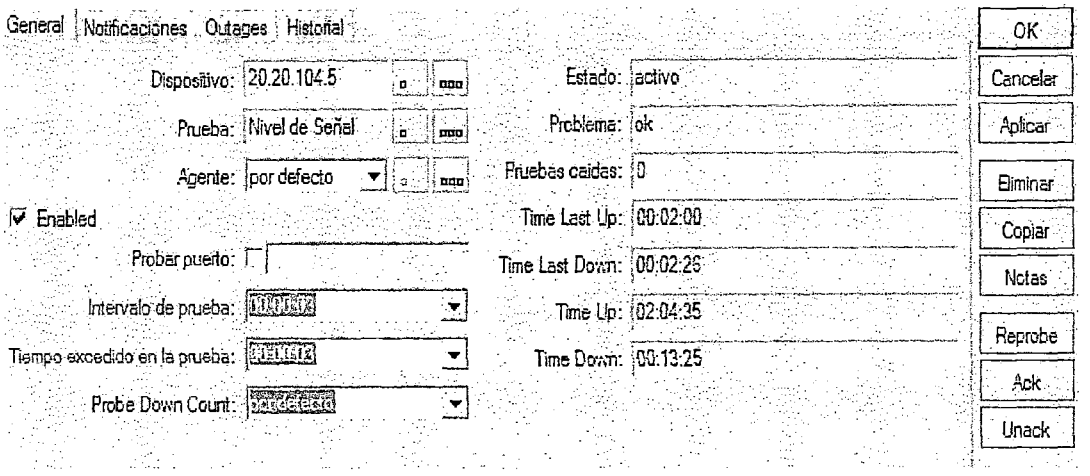


Ilustración 73 Ventana de Configuración de Intervalos de Prueba para el Parámetro de Nivel de Señal

- Luego en la pestaña **Notificaciones,** activamos con un check en "Use Notifications", y luego seleccionamos las siguientes notificaciones:

  Alarma por bajo nivel de señal en un enlace; con lo cual aparecerá el mensaje emergente creado en los pasos anteriores.

  Log to events; así tendremos el historial de las veces que los dispositivos presentaron este evento.

  Pitido; para darle sonido a la alarma.

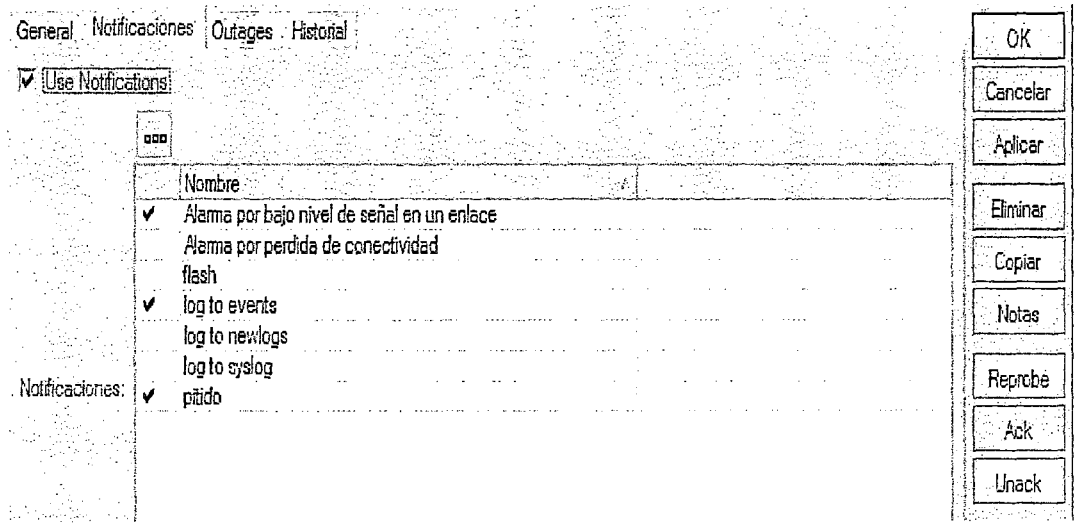


Ilustración 74 Ventana de Configuración de Notificaciones Para Alarma Por Bajo Nivel de Señal

El mensaje emergente se muestra de la siguiente manera:

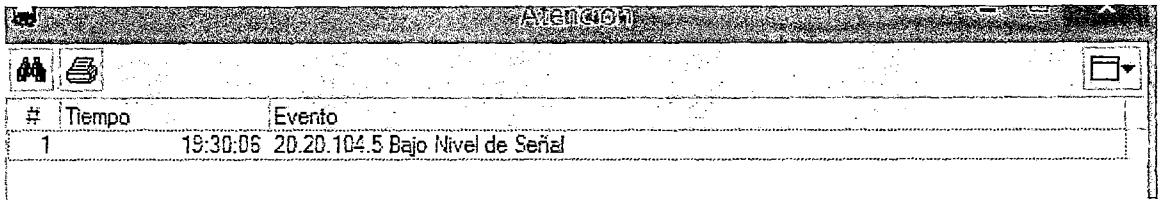


Ilustración 75 Mensaje Por Alarma de Bajo Nivel de Señal

Y el icono cambia de color demostrando tener una alarma presente:

Ilustración 76 Visualización de la Alarma por Bajo Nivel de Señal

También podemos ver el número de las veces, en que fechas ocurrieron, cuanto duro y cuál es el estado actual del evento

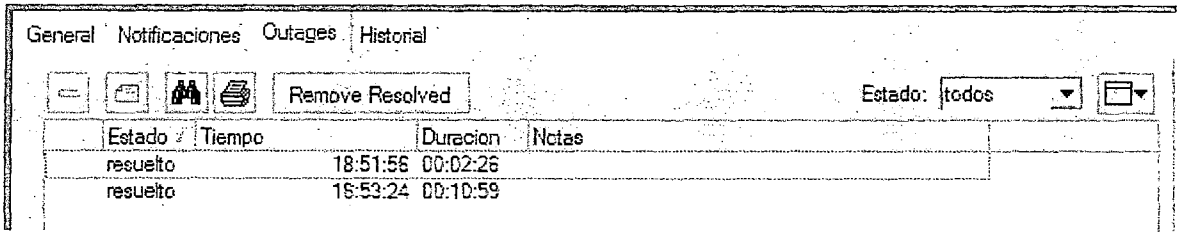


Ilustración 77 Historial de Registro de Alarma Por Bajo Nivel de Señal

c. Alarma por Alto uso de CPU y Memoria (A partir del 90%)

- Primero se creó una notificación con el mensaje emergente: "Alto uso de CPU".

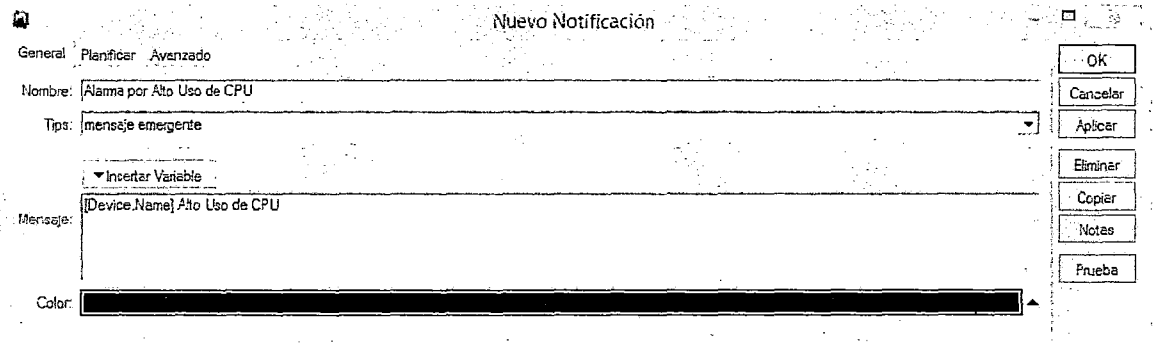


Ilustración 78 Ventana de Configuración de Notificación Para Alarma Por Alto uso de CPU

- Luego creamos una regla en la que indiquemos que si el uso de CPU o Memoria es mayor al 90% se active las notificaciones creadas para ello hicimos lo siguiente:
  - En la opción **Probes>+,** Llenamos los siguientes campos y clic en OK:

    Nombre: Uso de CPU

    Tips: SNMP, el protocolo por el cual obtenemos los datos.

    Oid: pegamos el OID correspondiente al uso de CPU.

    Tipo de Oid: Seleccionamos integer

    Método de Comparación: < = (menor o igual) se eligió esta opción por que esta se activa cuando la regla oid <= 90% es falsa.

    Valor Entero: 90,

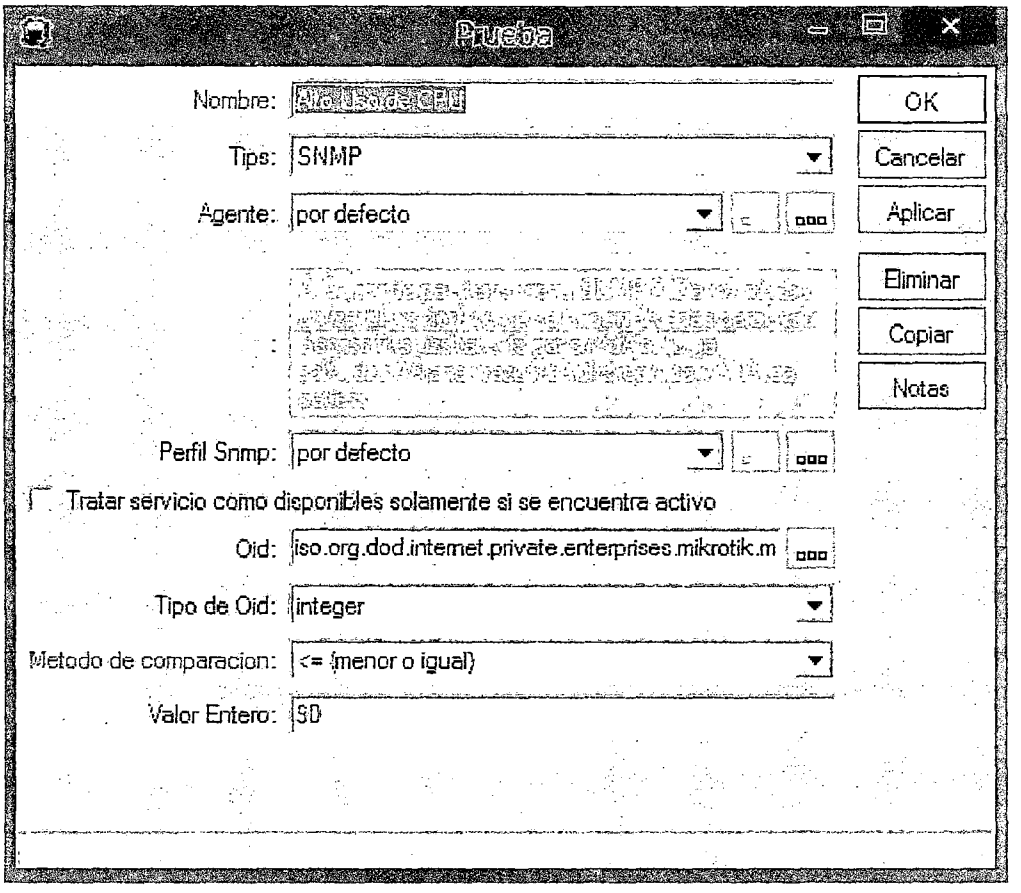


Ilustración 79 Ventana de Configuración de Uso de CPU

Teniendo creada la regla y la notificación procedemos a activarla y asociarlas, para ello realizamos lo siguiente.

- Doble clic en los dispositivos y en la pestaña general llenamos lo siguiente

  Prueba: Alto Uso de CPU

  Intervalo de prueba: 3 segundos

  Tiempo excedido en la prueba: 3 segundos

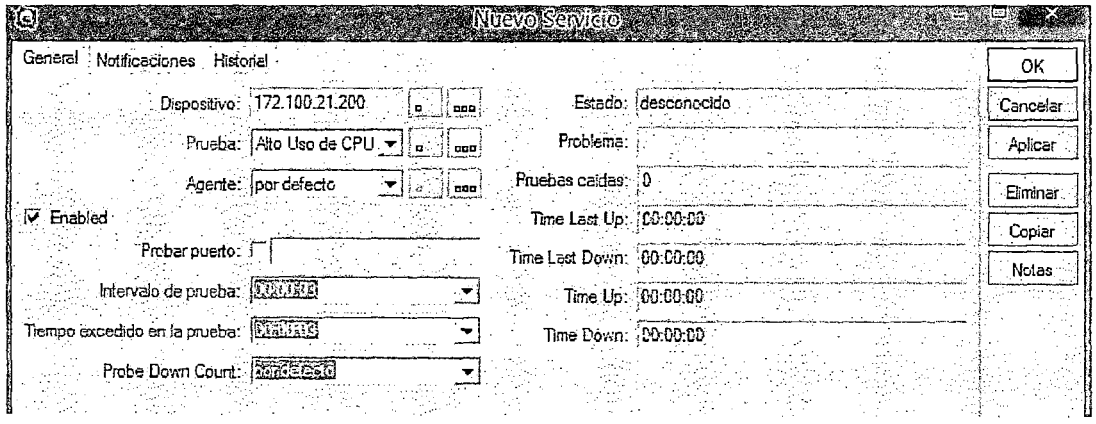


Ilustración 80 Ventana de Configuración de Intervalos de Prueba para el Parámetro de Uso de CPU

- Luego en la pestaña **Notificaciones,** activamos con un check en "Use Notifications", y luego seleccionamos las siguientes notificaciones:

  Alarma por Uso de CPU; con lo cual aparecerá el mensaje emergente creado en los pasos anteriores.

  Log to events; así tendremos el historial de las veces que los dispositivos presentaron este evento.

  Pitido; para darle sonido a la alarma.

El mensaje emergente se muestra de la siguiente manera:

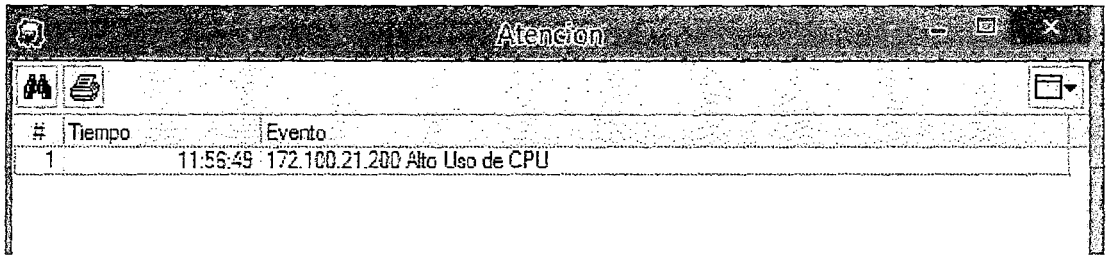


Ilustración 81 Mensaje Por Alarma de Alto Uso de CPU

d. Alarma por corte del suministro de Energía

Para la alarma de energía configuramos que cuando recibamos un trap este se visualice como mensaje emergente.

Para lo cual se crea la regla si no obtenemos un valor 1 del OID de alarma por corte de energía, lo que nos indica que se ha recibido un trab se active una notificación emergente.

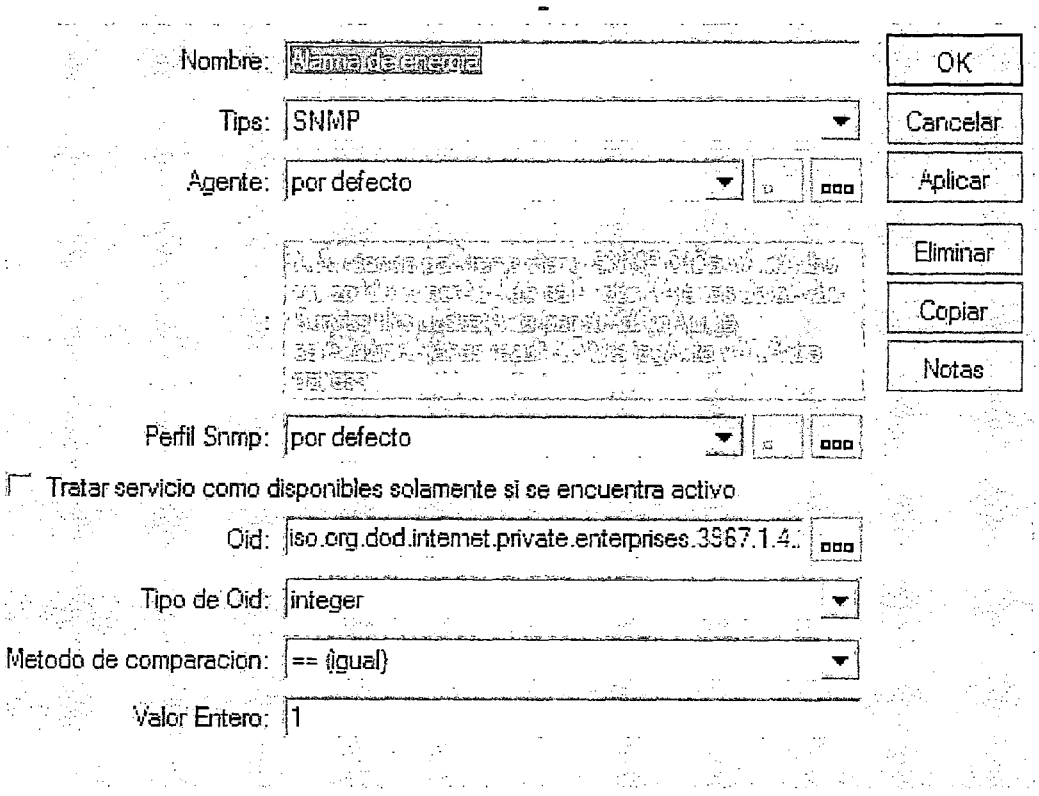


Ilustración 82 Creación de Alarma de Energia

Nombre: Alarma de energía

Tips: SNMP, el protocolo por el cual obtenemos los datos.

Oid: pegamos el OID correspondiente al trap de alarma por corte de energía.

Tipo de Oid: Seleccionamos integer

Método de Comparación: ==, se eligió esta opción por que esta se activa cuando la regla oid = 1 es falsa.

Valor Entero: 1,

Finalmente nos muestra el mensaje contenido en el trap recibido.

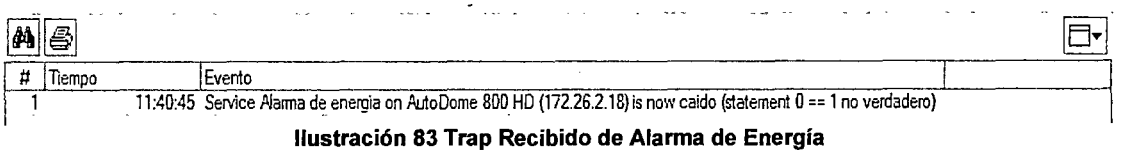


Ilustración 83 Trap Recibido de Alarma de Energía

5.2.6 Configuración de Servicios.

Dependiendo a la naturaleza de los dispositivos podemos hacer uso de múltiples servicios ofrecidos por este sistema, como nuestra red cuenta con componentes tales como cámaras y Access point, hemos optado por activar los acceso a sus interfaces web para facilitar las configuraciones remotas. Así también se decidió activar el servicio de envío de notificaciones vía email, pues para los administradores fue de suma importancia que no solo el personal de turno este enterado de los eventos si no todo el equipo responsable del área de soporte. A continuación se detalla lo realizado:

a. Servicio de Activación de la Interfaz Web

- Dentro del Software The Dude ingresamos a **Tools -> clic en +,** ingresamos los siguientes valores y clic en ok:

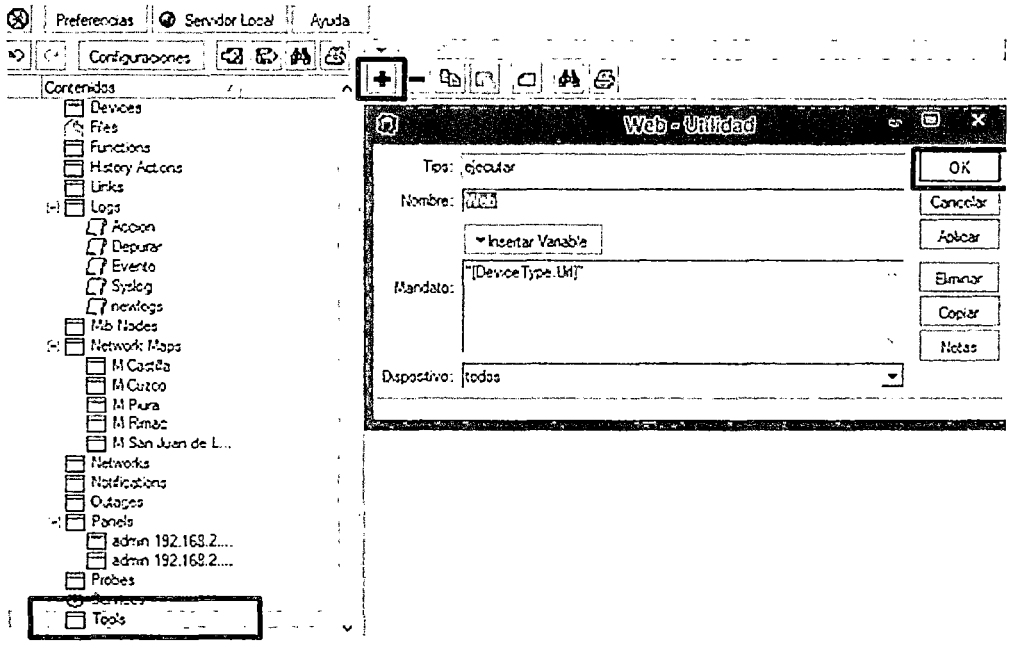


Ilustración 84 Creación del Servicio para acceso Web

- **Nombre:** Ingresamos **Web**
- **Mandato:** ingresamos el siguiente código **"[DeviceType.Url]"**
- **Dispositivos:** En esta opción seleccionamos **TODOS,** para así poder ingresar vía web a todos los dispositivos

- Como siguiente paso ingresamos las credenciales para cada equipo: **Clic Derecho sobre un elemento -> Configuraciones,** ingresamos el **usuario y contraseña** asignadas para este servicio **(Se creó un usuario SOPORTE para solo poder tener acceso a las configuraciones y mas no a las imágenes proporcionadas por las cámaras por motivos de seguridad)**

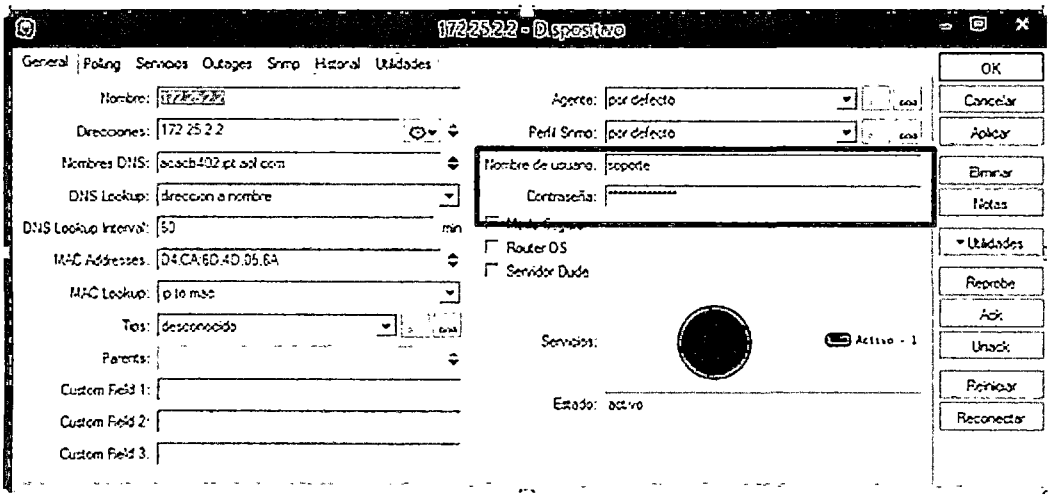


Ilustración 85 Configuración de Usuario para Accesos Web

- Para poder ingresar a la configuración vía web: **Clic derecho sobre un elemento -> Utilidades -> Web**

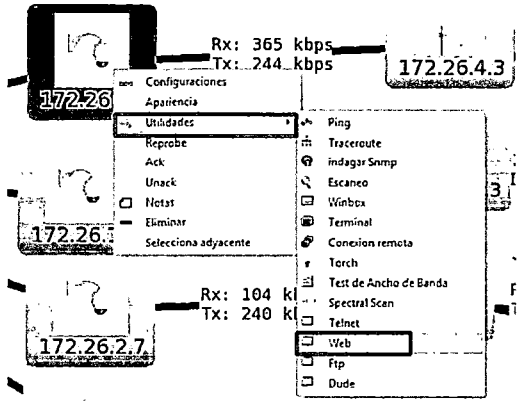


Ilustración 86 Procedimiento para el Acceso Web

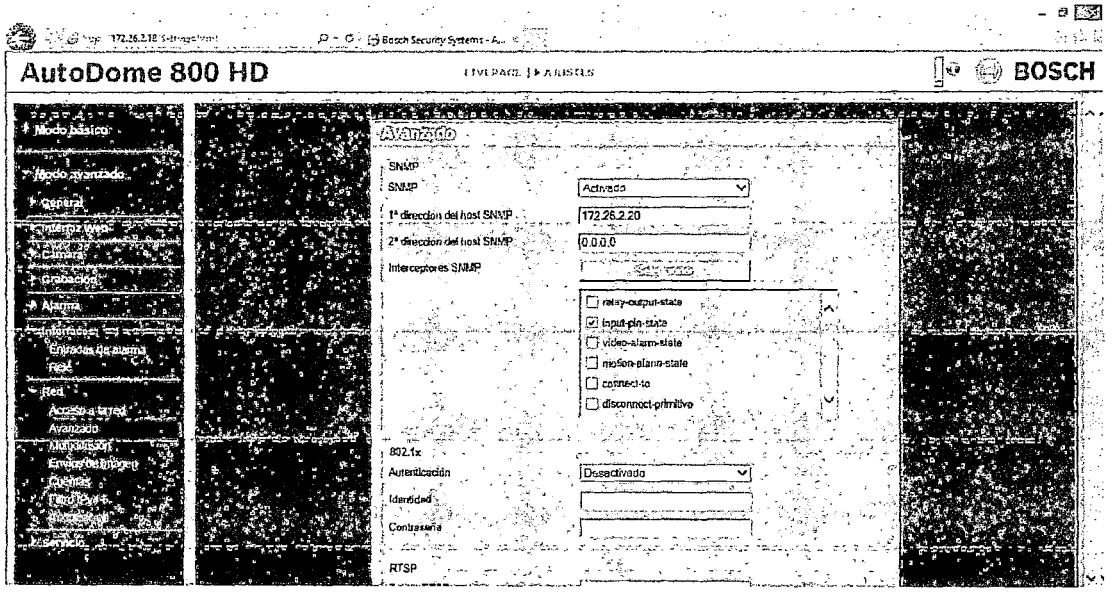


Ilustración 87 Acceso Web a una Cámara mediante The Dude

Ilustración 88 Acceso Web a una Radio mediante The Dude

b. Servicio de Notificación Vía Email

Se utilizó un programa como apoyo llamado "SendEmail" para el envío de las notificaciones, y un correo con dominio gmail.

El Programa SendEmail consta de los siguientes archivos:

SendEmail.exe, el cual permite la ejecución del programa de envío.

SendEmailxx2.cmd, en donde se configuran los parámetros de envío tales como el correo remitente y el correo destinatario, el SMTP server, el puerto SMTP entre otros.

set dir=c:\sendEmail

set smtpsender=soportenet@gmail.com

set smtpdst=soportenet@gmail.com

set smtpserver=smtp.gmail.com:465

set smtpport=25

set smtpuser= soportenet@gmail.com

set smtppwd=**********

"%dir%\sendEmail" -f %smtpsender% -t %smtpdst% -s %smtpserver% -u %smtpuser% -m %SERVIDOR THE DUDE ATENCION% -xp %smtppwd% -u

Creamos la notificación y la activamos en los dispositivos.

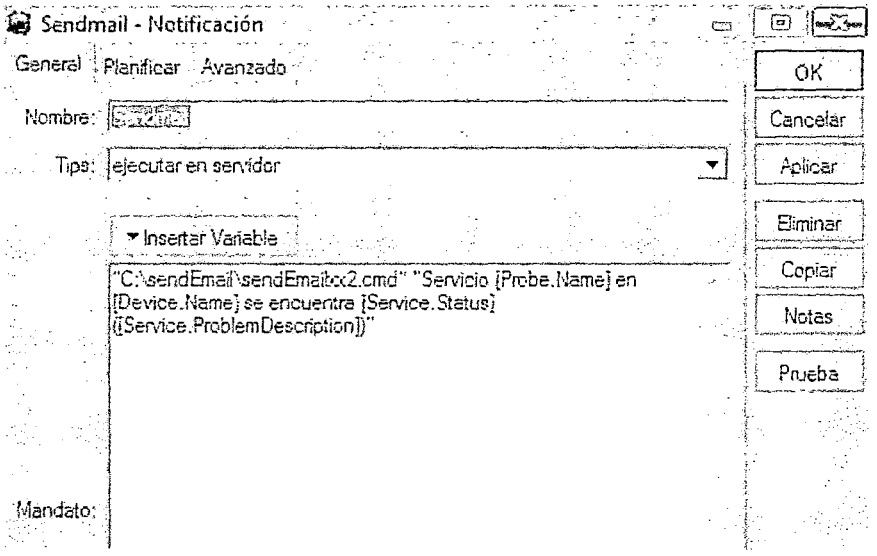


Ilustración 89 Ventana de Configuración de Notificación SendEmail

- **Nombre: Sendmail**
- **Tips:** ejecutar en servidor
- **Mandato:** Se ingresa el siguiente código: "C:\sendEmail\sendEmailxx2.cmd""Servicio [Probe.Name] en [Device.Name] se encuentra [Service.Status] ([Service.ProblemDescription])"
  En el cual se indica la ruta donde tenemos el programa SendEmail y el contenido del asunto del mail.

Finalmente se recibe el mensaje como se muestra en la imagen

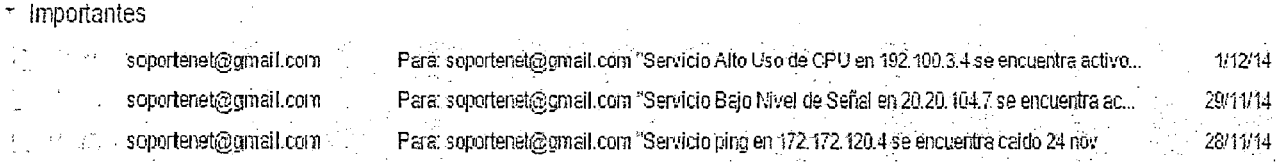


Ilustración 90 Notificación de Alarma Vía Email

CAPITULO VI

ANÁLISIS DE RESULTADOS

CAPITULO VI

ANÁLISIS DE RESULTADOS

El área de soporte de la empresa Netkrom Technologies, cuenta con un NOC para atención de 24 horas al día el cual se encarga de la recepción de informes de averías presentadas por los clientes (Municipalidades), dichas averías son reportadas por medios escritos (vía email) o medios hablados (vía telefónica). Después de recibir el reporte de avería el personal del NOC realiza las coordinaciones pertinentes para enviar personal técnico a sitio, estas visitas también son registradas, si el técnico necesita mayor material de lo llevado o nuevo personal esto también se registra como una segunda visita a sitio, luego utilizando la información dada por el técnico enviado proceden a clasificarlos en uno de los 4 grupos mapeados como tipos de averías, así tenemos:

Problemas de Hardware: Incluye, Problemas con la Cámaras o Radios, Problemas de Cableado, Problemas con los PoE, etc

Problemas Con Fluido Eléctrico: Incluye, Cortes de Energía, Problemas con el UPS.

Configuración de Cámara: Upgrades, pérdida de tours, etc.

Configuración de Radio: Saturación de Frecuencia, bajo nivel de señal, bajo CCQ, etc.

6.1 Número y Tipo de Averías Reportadas Antes De La Implementación Del Sistema Piloto.

a. El siguiente cuadro muestra las averías reportadas por la Municipalidad Del Rímac entre los meses de Enero y Agosto del 2014.

NÚMERO DE AVERÍAS REPORTADAS									
AVERÍAS \ MESES	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	TOTAL
Problemas de Hardware	0	1	0	3	1	1	2	2	10
Problema con Fluido Eléctrico	3	1	0	0	1	0	1	0	6
Configuración de Cámara	3	3	0	4	2	1	3	1	17
Configuración de Radio	5	1	2	0	2	1	2	1	14
TOTAL									47

Tabla 21 Averías Reportadas entre Enero – Agosto del 2014 en la M. Rímac

b. El siguiente cuadro muestra las averías reportadas por la Municipalidad de San Juan de Lurigancho entre los meses de Enero y Agosto del 2014.

NÚMERO DE AVERÍAS REPORTADAS									
AVERÍAS \ MESES	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	TOTAL
Problemas de Hardware	1	2	0	2	3	0	1	1	10
Problema con Fluido Eléctrico	1	0	1	1	0	2	0	1	6
Configuración de Cámara	2	2	3	2	0	2	1	2	14
Configuración de Radio	0	2	0	1	0	1	1	0	5
TOTAL									35

Tabla 22 Averías Reportadas entre Enero – Agosto del 2014 en la M. San Juan de Lurigancho

c. El siguiente cuadro muestra las averías reportadas por la Municipalidad de Piura entre los meses de Enero y Agosto del 2014.

NÚMERO DE AVERÍAS REPORTADAS									
AVERÍAS \ MESES	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	TOTAL
Problemas de Hardware	3	2	0	2	3	0	1	2	13
Problema con Fluido Eléctrico	1	0	1	1	0	2	0	2	7
Configuración de Cámara	2	2	2	3	1	3	1	4	18
Configuración de Radio	3	2	0	1	0	2	2	0	10
TOTAL									48

Tabla 23 Averías Reportadas entre Enero – Agosto del 2014 en la M. Piura

d. El siguiente cuadro muestra las averías reportadas por la Municipalidad de Castilla entre los meses de Enero y Agosto del 2014.

NÚMERO DE AVERÍAS REPORTADAS									
AVERÍAS \ MESES	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	TOTAL
Problemas de Hardware	1	2	2	2	3	0	1	2	13
Problema con Fluido Eléctrico	1	0	1	1	0	2	0	1	6
Configuración de Cámara	1	1	0	0	0	0	0	1	3
Configuración de Radio	0	1	0	1	1	1	1	0	5
TOTAL									27

Tabla 24 Averías Reportadas entre Enero – Agosto del 2014 en la M. Castilla

e. El siguiente cuadro muestra las averías reportadas por la Municipalidad de Cusco entre los meses de Enero y Agosto del 2014.

NÚMERO DE AVERÍAS REPORTADAS									
AVERÍAS \ MESES	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	TOTAL
Problemas de Hardware	0	2	0	2	1	0	1	2	8
Problema con Fluido Eléctrico	1	0	1	1	0	1	0	1	5
Configuración de Cámara	1	2	1	2	2	3	0	2	13
Configuración de Radio	0	1	0	1	0	1	3	0	6
TOTAL									32

Tabla 25 Averías Reportadas entre Enero – Agosto del 2014 en la M. Cusco

6.2 Número de **Visitas A Sitio Realizadas, Para Solucionar Averías Reportadas Antes De La Implementación Del Sistema Piloto**.

a. El siguiente cuadro indica las visitas a sitio para resolver las averías reportadas por la Municipalidad Del Rímac entre los meses de Enero y Agosto del 2014.

NÚMERO DE VISITAS A SITIO REGISTRADAS									
VISITAS \ MESES	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	TOTAL
Visitas a Sitio Por Problemas de Hardware	0	2	0	6	2	2	4	4	20
Visitas a Sitio Por Problema con Fluido Eléctrico	4	1	0	0	2	0	2	0	9
Visitas a Sitio Por Configuración de Cámara	3	3	0	4	2	1	3	1	17
Visitas a Sitio Por Configuración de Radio	5	1	2	0	2	1	2	1	14
TOTAL									60

Tabla 26 Visitas a Sitio entre Enero – Agosto del 2014 M. Rímac

b. El siguiente cuadro muestra las visitas a sitio para resolver las averías reportadas por la Municipalidad de San Juan de Lurigancho entre los meses de Enero y Agosto del 2014.

NÚMERO DE VISITAS A SITIO REGISTRADAS									
VISITAS \ MESES	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	TOTAL
Visitas a Sitio Por Problemas de Hardware	2	4	0	4	6	0	2	2	20
Visitas a Sitio Por Problema con Fluido Eléctrico	1	0	2	1	0	3	0	2	9
Visitas a Sitio Por Configuración de Cámara	2	2	3	2	0	2	1	2	14
Visitas a Sitio Por Configuración de Radio	0	2	0	1	0	1	1	0	5
TOTAL									48

Tabla 27 Visitas a Sitio entre Enero – Agosto del 2014 M. San Juan de Lurigancho

c. El siguiente cuadro muestra las visitas a sitio para resolver las averías reportadas por la Municipalidad de Piura entre los meses de Enero y Agosto del 2014.

NÚMERO DE VISITAS A SITIO REGISTRADAS									
VISITAS \ MESES	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	TOTAL
Visitas a Sitio Por Problemas de Hardware	6	4	0	4	6	0	2	4	26
Visitas a Sitio Por Problema con Fluido Eléctrico	2	0	1	2	0	3	0	2	10
Visitas a Sitio Por Configuración de Cámara	2	2	2	3	1	3	1	4	18
Visitas a Sitio Por Configuración de Radio	3	2	0	1	0	2	2	0	10
TOTAL									64

Tabla 28 Visitas a Sitio entre Enero – Agosto del 2014 M. Piura

d. El siguiente cuadro muestra las visitas a sitio para resolver las averías reportadas por la Municipalidad de Castilla entre los meses de Enero y Agosto del 2014.

NÚMERO DE VISITAS A SITIO REGISTRADAS									
VISITAS \ MESES	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	TOTAL
Visitas a Sitio Por Problemas de Hardware	2	4	4	4	6	0	2	4	26
Visitas a Sitio Por Problema con Fluido Eléctrico	1	0	2	2	0	3	0	1	9
Visitas a Sitio Por Configuración de Cámara	1	1	0	0	0	0	0	1	3
Visitas a Sitio Por Configuración de Radio	0	1	0	1	1	1	1	0	5
TOTAL									43

Tabla 29 Visitas a Sitio entre Enero – Agosto del 2014 M. Castilla

e. El siguiente cuadro muestra las visitas a sitio para resolver las averías reportadas por la Municipalidad de Cusco entre los meses de Enero y Agosto del 2014.

NÚMERO DE VISITAS A SITIO REGISTRADAS									
VISITAS \ MESES	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	TOTAL
Visitas a Sitio Por Problemas de Hardware	0	4	0	4	2	0	2	4	16
Visitas a Sitio Por Problema con Fluido Eléctrico	1	0	1	2	0	1	0	2	7
Visitas a Sitio Por Configuración de Cámara	1	2	1	2	2	3	0	2	13
Visitas a Sitio Por Configuración de Radio	0	1	0	1	0	1	3	0	6
TOTAL									42

Tabla 30 Visitas a Sitio entre Enero – Agosto del 2014 M. Cusco

6.3 Número y Tipo de Averías Reportadas Después De La Implementación Del Sistema Piloto.

a. El siguiente cuadro muestra las averías reportadas por la Municipalidad Del Rímac entre los meses de Setiembre a Diciembre del 2014 y Enero del 2015.

NÚMERO DE AVERÍAS REPORTADAS						
AVERÍAS \ MESES	Setiembre	Octubre	Noviembre	Diciembre	Enero	TOTAL
Problemas de Hardware	1	2	0	3	2	8
Problema con Fluido Eléctrico	0	1	1	0	1	3
Configuración de Cámara	2	2	1	1	2	8
Configuración de Radio	2	1	2	0	0	5
TOTAL						24

Tabla 31 Averías Reportadas entre Septiembre del 2014 – Enero del 2015 en la M. Rímac

b. El siguiente cuadro muestra las averías reportadas por la Municipalidad de San Juan de Lurigancho entre los meses de Setiembre a Diciembre del 2014 y Enero del 2015.

NÚMERO DE AVERÍAS REPORTADAS						
AVERÍAS \ MESES						
Problemas de Hardware	0	1	1	3	1	6
Problema con Fluido Eléctrico	2	1	0	0	1	4
Configuración de Cámara	1	3	1	4	2	11
Configuración de Radio	1	1	2	0	1	5
TOTAL						26

Tabla 32 Averías Reportadas entre Septiembre del 2014 – Enero del 2015 en la M. San Juan de Lurigancho

c. El siguiente cuadro muestra las averías reportadas por la Municipalidad de Piura entre los meses de Setiembre a Diciembre del 2014 y Enero del 2015.

NUMERO DE AVERIAS REPORTADAS						
AVERÍAS \ MESES						
Problemas de Hardware	0	1	1	3	1	6
Problema con Fluido Electrico	2	1	0	1	1	5
Configuración de Cámara	1	2	1	4	2	10
Configuración de Radio	1	1	2	0	0	4
TOTAL						25

Tabla 33 Averías Reportadas entre Septiembre del 2014 – Enero del 2015 en la M. Piura

d. El siguiente cuadro muestra las averías reportadas por la Municipalidad de Castilla entre los meses de Setiembre a Diciembre del 2014 y Enero del 2015.

NUMERO DE AVERIAS REPORTADAS						
AVERÍAS \ MESES						
Problemas de Hardware	0	1	0	3	1	5
Problema con Fluido Electrico	2	1	0	0	1	4
Configuración de Cámara	1	2	0	2	2	7
Configuración de Radio	2	1	2	0	2	7
TOTAL						23

Tabla 34 Averías Reportadas entre Septiembre del 2014 – Enero del 2015 en la M. Castilla

e. El siguiente cuadro muestra las averías reportadas por la Municipalidad de Cusco entre los meses de Setiembre a Diciembre del 2014 y Enero del 2015.

NÚMERO DE AVERÍAS REPORTADAS						
AVERÍAS \ MESES						
Problemas de Hardware	0	1	0	3	2	6
Problema con Fluido Eléctrico	2	1	0	0	1	4
Configuración de Cámara	1	3	0	4	2	10
Configuración de Radio	1	1	2	0	0	4
TOTAL						24

Tabla 35 Averías Reportadas entre Septiembre del 2014 – Enero del 2015 en la M. Cusco

6.4 Número Visitas A Sitio Realizadas Para Solucionar Averías Reportadas Después De La Implementación Del Sistema Piloto.

a. El siguiente cuadro muestra las visitas a sitio para resolver las averías reportadas por la Municipalidad Del Rímac entre los meses de Setiembre a Diciembre del 2014 y Enero del 2015.

NÚMERO DE VISITAS A SITIO REGISTRADAS						
VISITAS \ MESES						
Problemas de Hardware	2	3	0	3	2	10
Problema con Fluido Eléctrico	0	2	1	0	1	4
Configuración de Cámara	2	1	1	0	1	5
Configuración de Radio	2	1	0	0	0	3
TOTAL						22

Tabla 36 Visitas a Sitio Realizadas entre Septiembre del 2014 – Enero del 2015 en la M. Rímac

b. El siguiente cuadro muestra las visitas a sitio para resolver las averías reportadas por la Municipalidad de San Juan de Lurigancho entre los meses de Setiembre a Diciembre del 2014 y Enero del 2015.

NÚMERO DE VISITAS A SITIO REGISTRADAS						
VISITAS \ MESES						
Problemas de Hardware	0	2	1	3	1	7
Problema con Fluido Eléctrico	3	1	0	0	1	5
Configuración de Cámara	1	2	0	1	0	4
Configuración de Radio	1	1	1	0	0	3
TOTAL						19

Tabla 37 Visitas a Sitio Realizadas entre Septiembre del 2014 – Enero del 2015 en la M. San Juan de Lurigancho

c. El siguiente cuadro muestra las visitas a sitio para resolver las averías reportadas por la Municipalidad de Piura entre los meses de Setiembre a Diciembre del 2014 y Enero del 2015.

NÚMERO DE VISITAS A SITIO REGISTRADAS						
VISITAS \ MESES						
Problemas de Hardware	0	2	1	3	1	7
Problema con Fluido Eléctrico	3	1	0	1	1	6
Configuración de Cámara	1	1	1	1	0	4
Configuración de Radio	1	0	0	0	0	1
TOTAL						18

Tabla 38 Visitas a Sitio Realizadas entre Septiembre del 2014 – Enero del 2015 en la M. Piura

d. El siguiente cuadro muestra las visitas a sitio para resolver las averías reportadas por la Municipalidad de Castilla entre los meses de Setiembre a Diciembre del 2014 y Enero del 2015.

NÚMERO DE VISITAS A SITIO REGISTRADAS						
VISITAS \ MESES						
Problemas de Hardware	0	2	0	3	1	6
Problema con Fluido Electrico	3	2	0	0	1	6
Configuración de Cámara	1	1	0	0	1	3
Configuración de Radio	1	0	1	0	0	2
TOTAL						17

Tabla 39 Visitas a Sitio Realizadas entre Septiembre del 2014 – Enero del 2015 en la M. Castilla

e. El siguiente cuadro muestra las visitas a sitio para resolver las averías reportadas por la Municipalidad de Cusco entre los meses de Setiembre a Diciembre del 2014 y Enero del 2015.

NÚMERO DE VISITAS A SITIO REGISTRADAS						
VISITAS \ MESES						
Problemas de Hardware	0	2	0	3	2	7
Problema con Fluido Electrico	2	2	0	0	1	5
Configuración de Cámara	0	1	0	1	0	2
Configuración de Radio	1	0	1	0	0	2
TOTAL						16

Tabla 40 Visitas a Sitio Realizadas entre Septiembre del 2014 – Enero del 2015 en la M. Cusco

6.5 Análisis de Las Gráficas de Visitas a Sitio vs El Número de Averías Reportadas.

De acuerdo a los cuadros presentados concluimos que antes de la implementación del sistema piloto el número de visitas a sitio para solucionar averías era mayor al número de averías reportadas teniendo este resultado por diferentes casos tales como:

Al no contar con la información necesaria de la avería la empresa manda un técnico a verificar el caso y muchas veces se trata de corte de fluido eléctrico y dicho problema no es responsabilidad de la empresa atender, por ende no debería haber movilizado personal en esa instancia, pero después de recuperado el corte muchas veces se presentan problemas con le UPS o los PoE y en este caso la empresa si tiene que ir a sitio, pero en vez de que sea solo una visita, ya hemos reportado dos. Otro caso presentado es cuando el técnico enviado que está capacitado solo en mantenimiento de hardware, llegando a sitio se da cuenta que el problema que tiene que atender es de configuración, por ende reporta que se necesita enviar personal especializado por lo cual volvemos a reportar dos visitas por un mismo caso, y estos son solo algunos ejemplos de los muchos casos que se presentan y que terminar con dos o tres visitas a sitio, cuando solo se debería reportar una única visita.

En las municipalidades de Cusco y Castilla después del primer mes de la implementación del Sistema piloto se vio una notoria disminución de las visitas a sitio, esto fue por la gran colaboración que se tubo de parte del personal de las municipalidades los cuales nos apoyaron completamente con las pruebas del sistema y es así que cada caso referente a configuración se pudo solucionar remotamente.

En caso de las municipalidades de San Juan de Lurigancho, Piura y el Rímac la disminución de visitas a sitio se dio a notar a partir del segundo a tercer mes de instalado el sistema piloto esto se debió mayormente a la costumbre del cliente de requerir ver a un personal en sitio trabajando en la resolución de su avería, pero poco a poco se fue tratando de liberar esa idea, y es así que ya en el mes de noviembre se pudo concretar las pruebas y lograr que las configuraciones se resuelvan de forma remota y también se logró ayudar a diagnosticar la ubicación exacta de las fallas.

Los siguientes cuadros nos muestran gráficamente el comportamiento relatado:

a. Municipalidad del Rímac

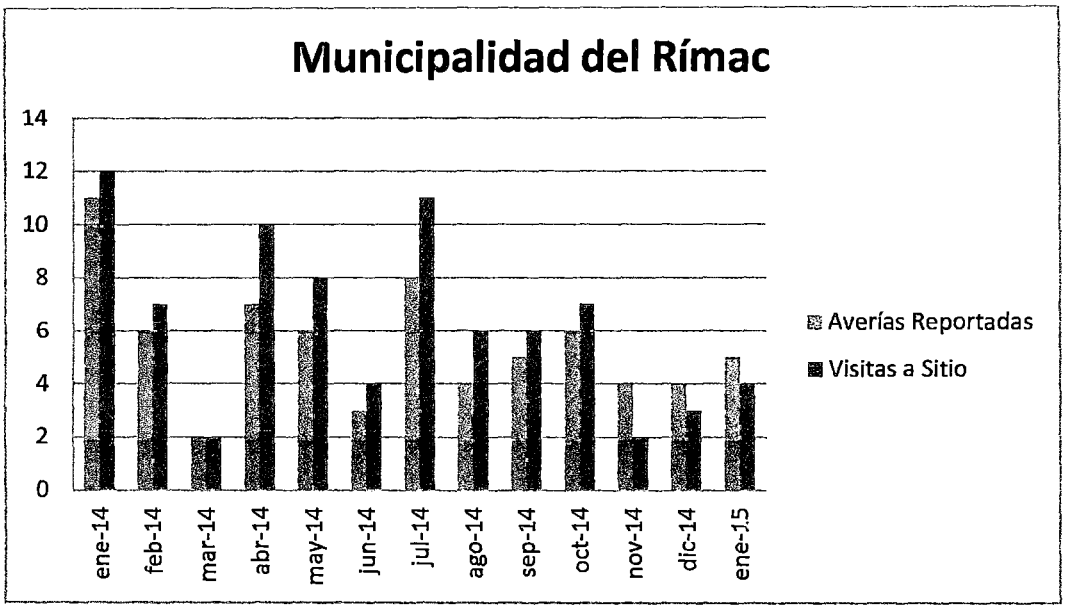


Ilustración 91 Visitas a Sitio vs Número de Averías M. Rímac

b. Municipalidad de San Juan de Lurigancho.

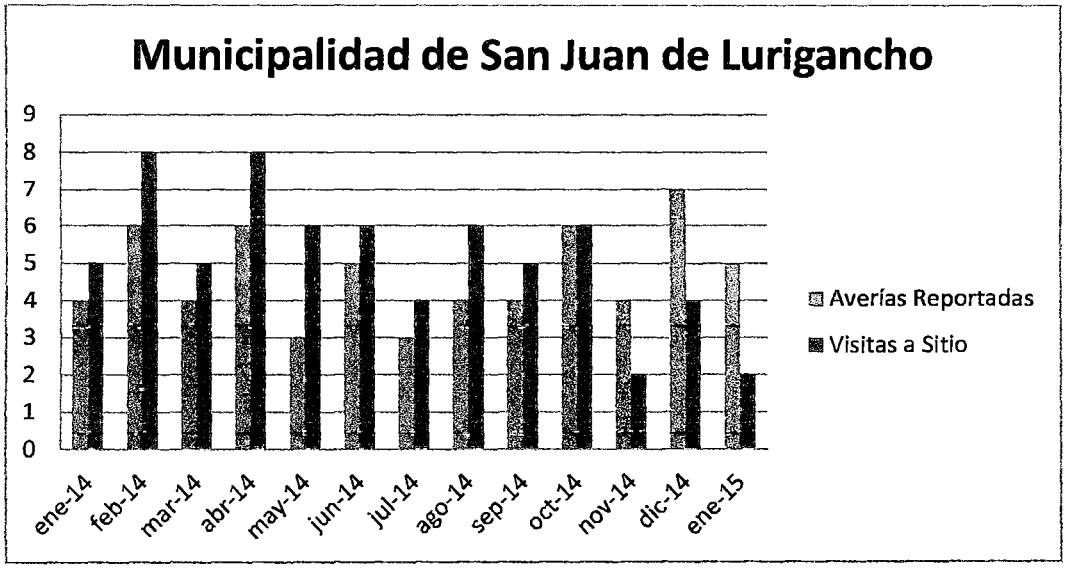


Ilustración 92 Visitas a Sitio vs Número de Averías M. San Juan de Lurigancho

c. Municipalidad de Piura

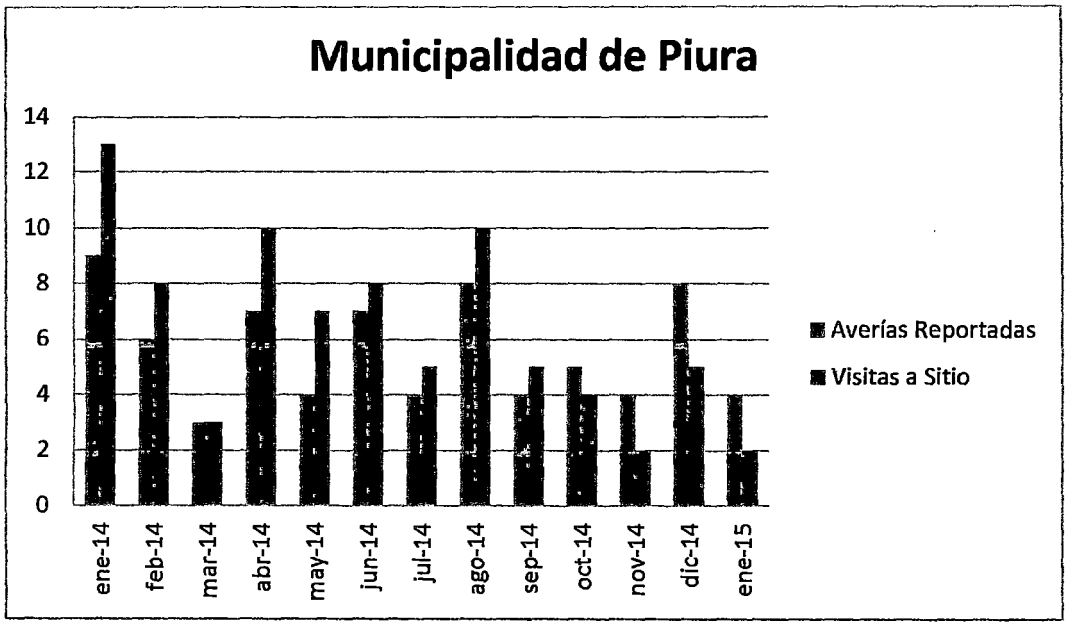


Ilustración 93 Visitas a Sitio vs Número de Averías M. Piura

d. Municipalidad de Castilla

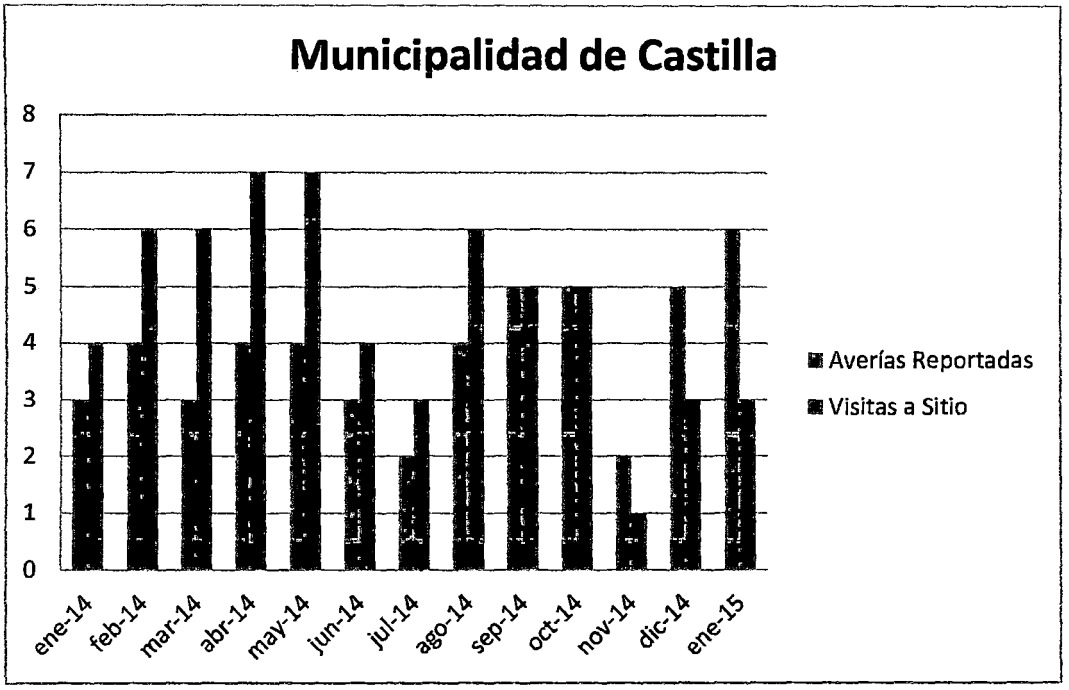


Ilustración 94 Visitas a Sitio vs Número de Averías M. Castilla

e. Municipalidad de Cusco

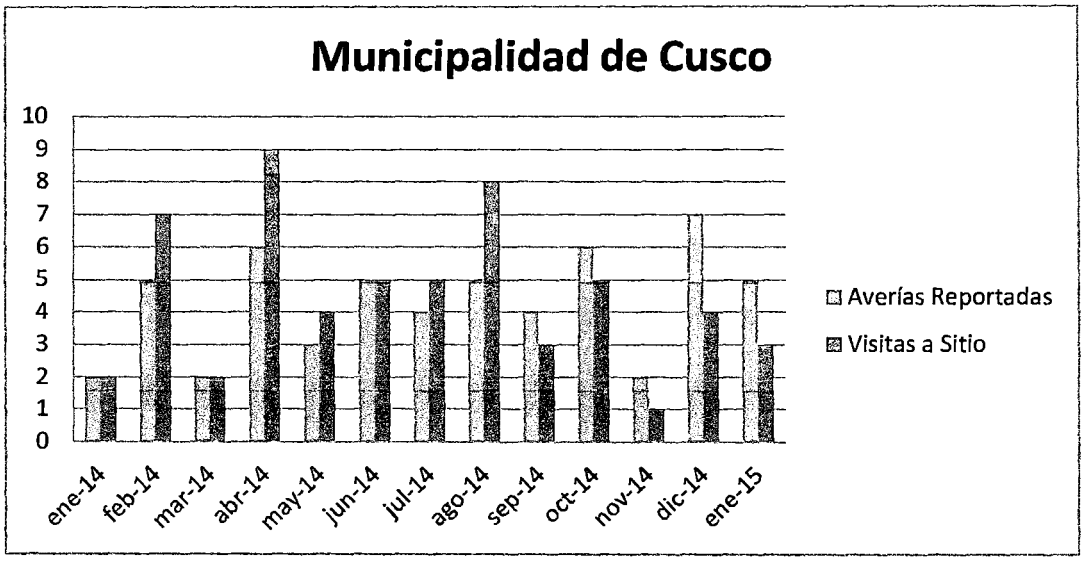


Ilustración 95 Visitas a Sitio vs Número de Averías M. Cusco

6.6 Casos Fuera de los Tiempo de Respuesta establecidos en el SLA

Los tiempos de respuesta establecidos en el contrato dependen de la avería reportada, así tenemos:

Para Problemas de Hardware

- Diagnóstico: 1h
- Primer Update de Solución: 2h después del Diagnóstico
- Segundo Update de Solución: 2h después del Primer Update
- Solución del Problema: 3h después del Segundo Update

Haciendo un total de 8 horas para su solución

Para Problemas de Configuración

- Diagnóstico: 30 minutos
- Update de Solución: 1h después del Diagnóstico
- Solución del Problema: 2h y 30minutos después del Update

En caso de los clientes ubicados en provincias a estos tiempos se les sumaba el tiempo de viaje vía aérea a la provincia donde se encontraban ubicados.

Haciendo un total de 4 horas para su solución

6.6.1 Antes De La Implementación Del Sistema Piloto.

En las siguientes tablas se muestra el número de veces que la empresa no ha podido cumplir con los tiempos de respuesta establecidos en los contratos de SLA, esto es otra consecuencia de los problemas ya expuestos anteriormente, y que con lleva a un nuevo problema que sumado a las multas que tiene que asumir la empresa, es la mala imagen que esta se está fomentando con sus clientes al no cumplir con dichos contratos de SLA.

Casos Fuera de los Tiempo de Respuesta establecidos en SLA									
Municipalidades \ MESES	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Total
M. Rímac	5	4	1	3	3	1	3	2	22
M. San Juan de Lurigancho	2	4	1	3	1	3	1	2	17
M. Piura	6	4	2	4	2	4	2	5	29
M. Castilla	2	2	1	2	2	1	2	3	15
M. Cusco	1	4	1	5	1	3	2	3	20

Tabla 41 Casos Fuera del SLA Antes de la implementación del Sistema Piloto

De los gráficos podemos concluir que los clientes con los que más se incurre en falta son los que se ubican en provincia, algo que es muy lógico habiendo analizado que en muchos ocasiones se necesitaba más de una visita por el mismo caso y teniendo en cuenta la distancia hacia dichos sitios es difícil estar dentro de los tiempos de respuesta requeridos.

a. Municipalidad del Rímac

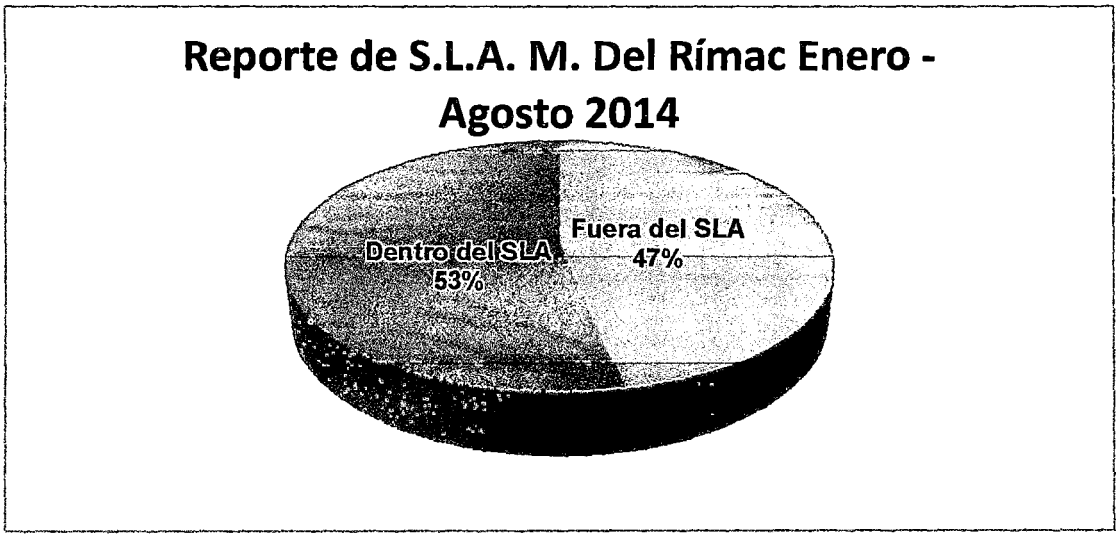


Ilustración 96 Reporte de S.L.A. M. Del Rímac Enero - Agosto 2015

b. Municipalidad de San Juan de Lurigancho.

Ilustración 97 Reporte de S.L.A. M. De San Juan de Lurigancho Enero - Agosto 2015

c. Municipalidad de Piura

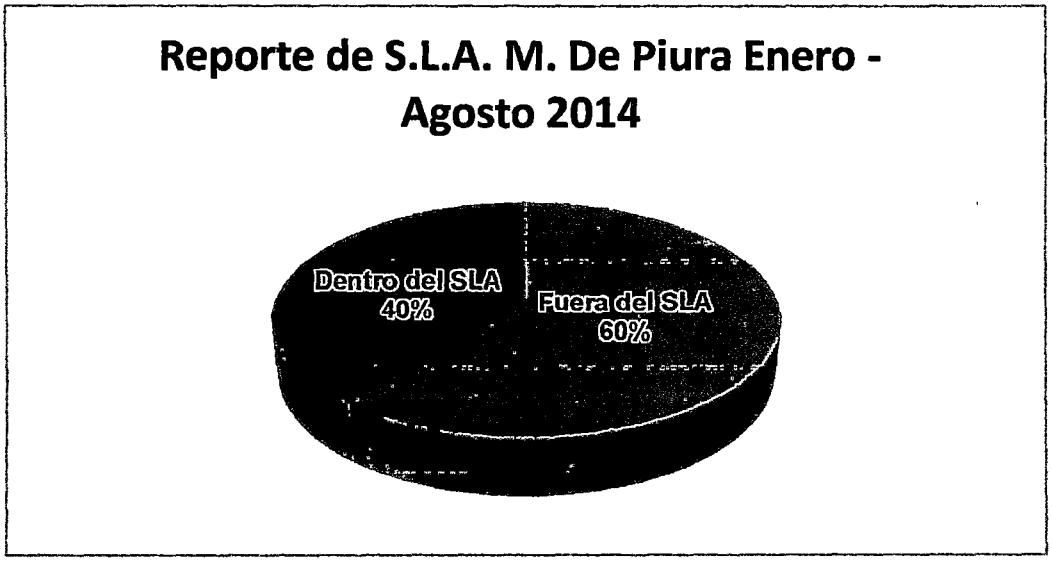


Ilustración 98 Reporte de S.L.A. M. De Piura Enero - Agosto 2015

d. Municipalidad de Castilla

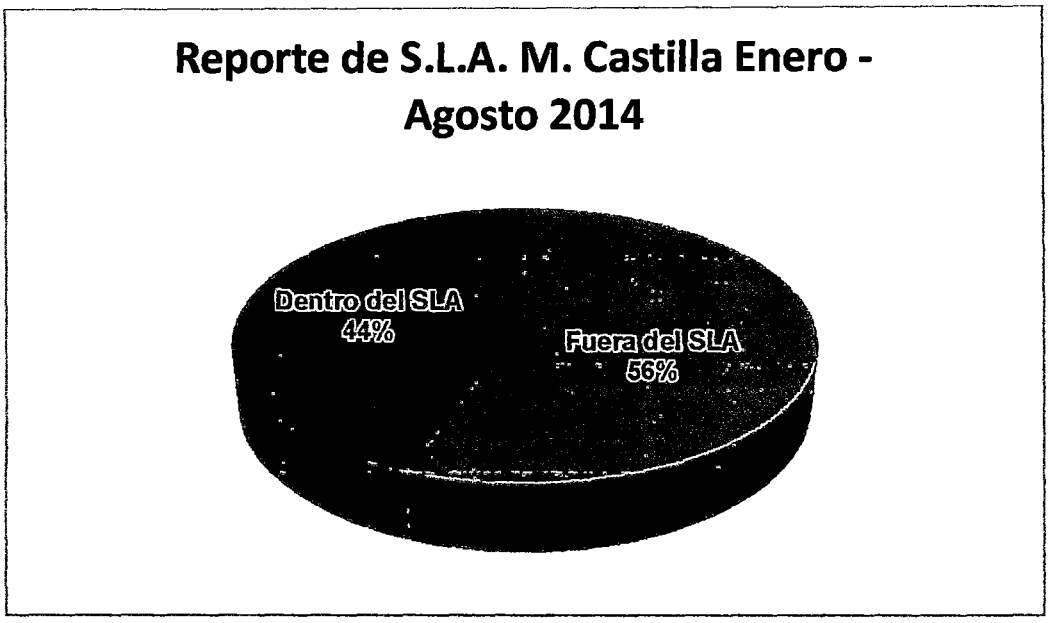


Ilustración 99 Reporte de S.L.A. M. Castilla Enero - Agosto 2014

e. Municipalidad de Cusco

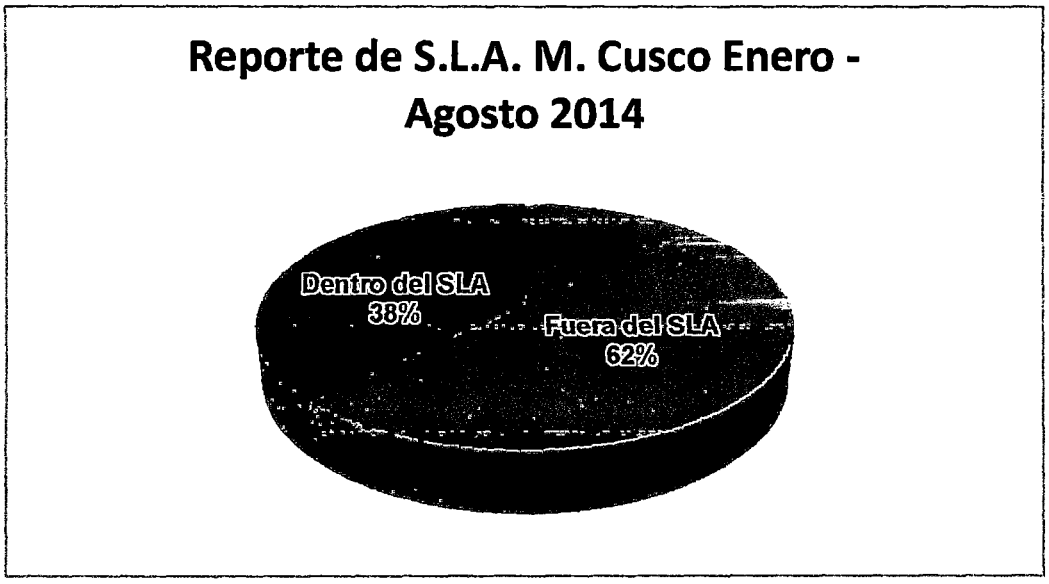


Ilustración 100 Reporte de S.L.A. M. Cusco Enero - Agosto 2014

6.6.2 Después De La Implementación Del Sistema Piloto.

Después de la Implementación del sistema se logró reducir los casos que salían de los SLA establecidos, los resultados fueron bastantes favorables sobre todo para los clientes ubicados en provincia, esto fue a consecuencia de que la mayoría de los problemas relacionados a configuración de radio y cámara se resolvieron de forma remota y es así que reducimos el tiempo significativamente, logrando así una gran satisfacción de dichos clientes con el nuevo sistema.

Casos Fuera de los Tiempo de Respuesta establecidos en SLA						
Municipalidades \ MESES	Setiembre	Octubre	Noviembre	Diciembre	Enero	TOTAL
M. Rímac	3	3	1	1	2	10
M. San Juan de Lurigancho	2	3	1	2	1	9
M. Piura	2	2	1	2	0	7
M. Castilla	1	1	0	1	1	4
M. Cusco	1	1	0	1	1	4

Tabla 42 Casos Fuera del SLA Después de la Implementación del Sistema Piloto

Las siguientes imágenes muestran gráficamente el comportamiento relatado:

a. Municipalidad del Rímac

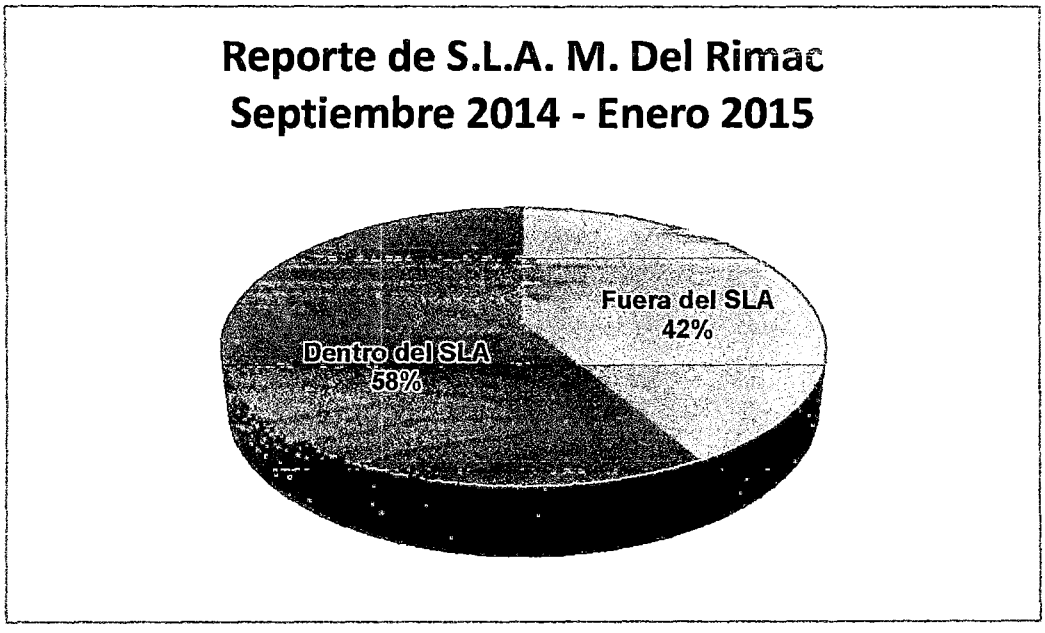


Ilustración 101 Reporte de S.L.A. M. Del Rímac Septiembre 2014 - Enero 2015

b. Municipalidad de San Juan de Lurigancho.

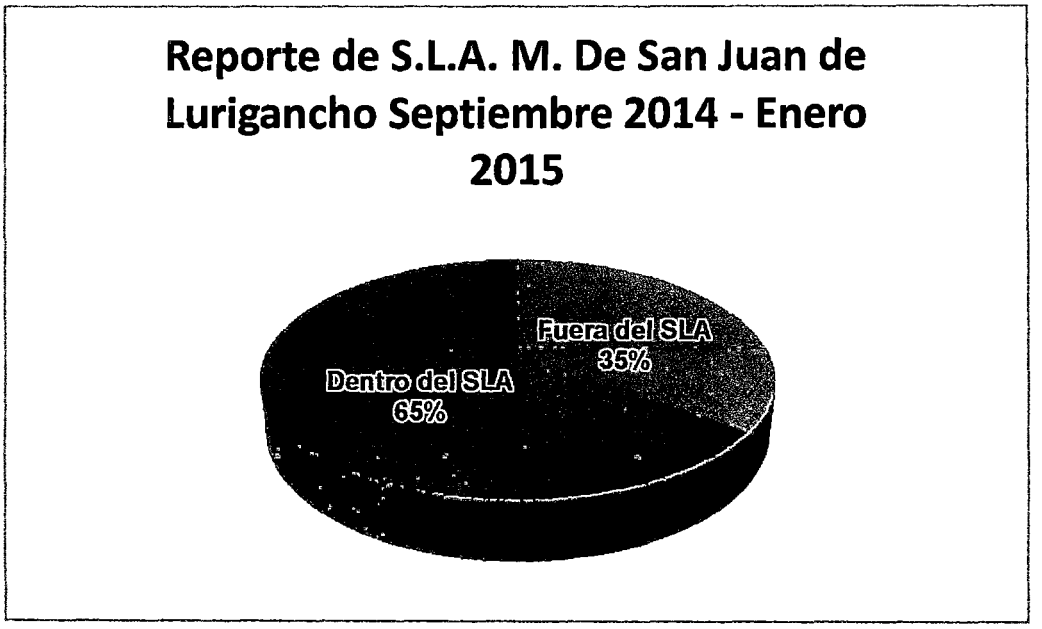


Ilustración 102 Reporte de S.L.A. M. De San Juan de Lurigancho Septiembre 2014 - Enero 2015

c. Municipalidad de Piura

Ilustración 103 Reporte de S.L.A. M. De Piura Septiembre 2014 - Enero 2015

d. Municipalidad de Castilla

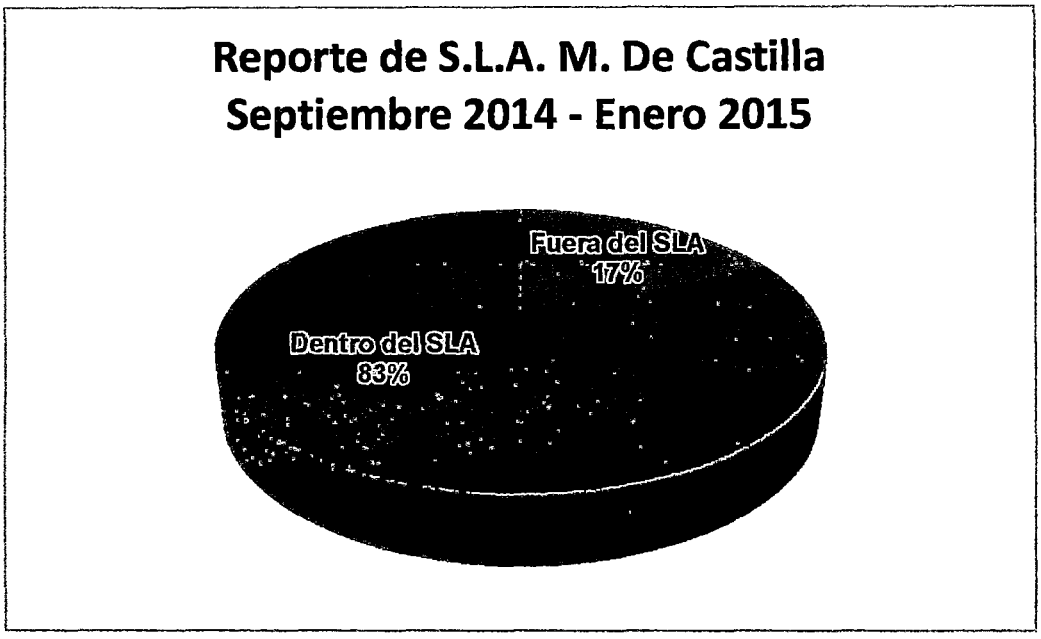


Ilustración 104 Reporte de S.L.A. M. De Castilla Septiembre 2014 - Enero 2015

e. Municipalidad de Cusco

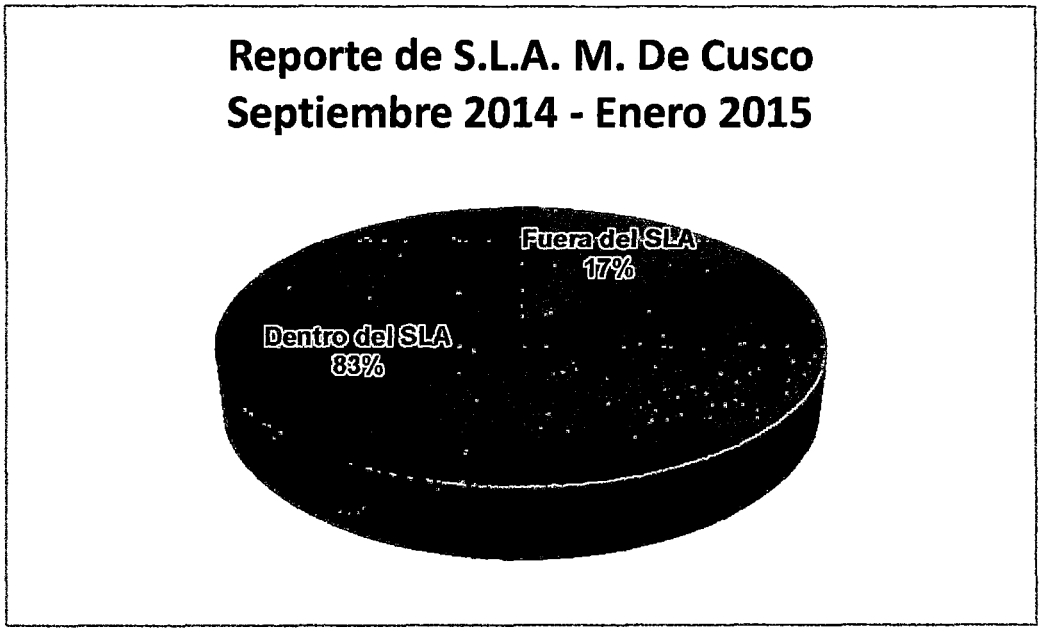


Ilustración 105 Reporte de S.L.A. M. De Cusco Septiembre 2014 - Enero 2015

CAPITULO VII

ESTUDIO ECONÓMICO

CAPÍTULO VII

ESTUDIO ECONÓMICO

7.1 Presupuesto General

Los precios que a continuación se muestran, son precios obtenidos actualmente de diferentes empresas del mercado local, incluyendo el IGV.

Las marcas de los equipos fueron elegidas por la familiaridad de los usuarios con dichas marcas teniendo en cuenta las características recomendadas por los autores, que permitan el buen funcionamiento del sistema.

7.1.1 Sistema de VPNs.

A continuación se presenta el presupuesto de los Equipos necesarios para la implementación del sistema de VPNs.

Ítem	Descripción	Cantidad	Precio Unidad	Precio Total
1	RouterBoard MIKROTIK 1100AH x2	1	S/. 2,000.00	S/. 2,000.00
2	RouterBoard MIKROTIK 750 GL	5	S/. 350.00	S/. 1,750.00
3	Patch Cord CAT5 de 3mts c/u	16	S/. 12.00	S/. 192.00
	TOTAL			**S/. 3,942.00**

Tabla 43 Presupuesto del Sistema de VPNs

7.1.2 Sistema de Gestión y Monitoreo.

A continuación se presenta el presupuesto de los Equipos necesarios para la implementación del sistema de Gestión y Monitoreo.

Ítem	Descripción	Cantidad	Precio Unidad	Precio Total
1	PC HP Compaq 6300 Pro SFF	1	S/. 3,500.00	S/. 3,500.00
2	Teclado+ Mouse Microsoft Inalámbrico	1	S/. 150.00	S/. 150.00
3	Supresor de Picos Forza 220V.	1	S/. 25.00	S/. 25.00
4	Estabilizador APC 1200va	1	S/. 500.00	S/. 500.00
5	Smart- UPS APC C1000	1	S/. 2,300.00	S/. 2,300.00
6	Monitores LCD 42" LG	2	S/. 1,800.00	S/. 3,600.00
7	Cables HDMI 3mts c/u	2	S/. 25.00	S/. 50.00
8	Rack de Pared para TV de 42"	2	S/. 200.00	S/. 400.00

9	Tarjeta de Video ASUS NVIDIA GeForce GT 630, 2 GB GDDR3, HDMI, DVI. Puerto PCI Express 2.0.	1	S/. 800.00	S/. 800.00
	TOTAL			**S/. 11,325.00**

Tabla 44 Presupuesto del Sistema de Gestión y Monitoreo

7.1.3 Mano de Obra.

A continuación se presenta el presupuesto de la mano de obra tanto para la instalación del Sistema de VPN como del Sistema de Gestión y Monitoreo.

Ítem	Descripción	Precio Unidad
1	Instalación del Sistema de VPN Cliente en la M. del Rímac	S/. 800.00
2	Instalación del Sistema de VPN Cliente en la M. de San Juan de Lurigancho	S/. 800.00
3	Instalación del Sistema de VPN Cliente en la M. de Piura	S/. 1,200.00
4	Instalación del Sistema de VPN Cliente en la M. de Castilla	S/. 1,200.00
5	Instalación del Sistema de VPN Cliente en la M. de Cusco	S/. 1,200.00
6	Instalación del Sistema de VPN Servidor.	S/. 800.00
7	Instalación del Sistema de Gestión y Monitoreo	S/. 2,000.00
	TOTAL	**S/. 8,000.00**

Tabla 45 Costo de Mano de Obra de Todo el Proyecto

7.1.4 Costo Total de La Inversión.

Como se puede observar el costo total de inversión asciende a un monto de **VEINTITRÉS MIL DOSCIENTOS SESENTA Y SIETE NUEVOS SOLES**

Ítem	Descripción	Precio Unidad
1	Presupuesto del Sistema de VPN	S/. 3,942.00
2	Presupuesto del Sistema de Gestión y Monitoreo	S/. 11,325.00
3	Mano de Obra	S/. 8,000.00
	TOTAL	**S/. 23,267.00**

Tabla 46 Costo Total del Proyecto

7.2 Análisis de Retorno de Inversión

7.2.1 Egresos Por Visita a Sitio.

A continuación se detalla los Egresos de la Empresa por cada visita a sitio realizada.

a. Egresos de clientes ubicados en Lima.

Ítem	Descripción	Precio Unidad
1	Pago a Técnico	S/. 70.00
2	Pago a Ingeniero	S/. 100.00
3	Movilidad	S/. 30.00
TOTAL		**S/. 200.00**

Tabla 47 Egresos de clientes ubicados en Lima por Visita a Sitio

b. Egresos de clientes ubicados en Provincia.

Ítem	Descripción	Precio Unidad
1	Pago a Técnico	S/. 70.00
2	Pago a Ingeniero	S/. 100.00
3	Movilidad (avión)	S/. 700.00
3	Viáticos	S/. 80.00
TOTAL		**S/. 950.00**

Tabla 48 Egresos de clientes ubicados en Provincia por Visita a Sitio

7.2.2 Egresos Mensuales Promedio.

En el siguiente cuadro se detalla los Egresos Mensuales promedio por visitas a sitio.

a. Egresos mensuales antes de la implementación del sistema piloto.

Descripción	Cantidad	Costo Unidad	Costo Total
Número promedio de visitas a sitio por mes en Lima	14	S/. 200.00	S/. 2,800.00
Número promedio de visitas a sitio por mes en Provincia	19	S/. 950.00	S/. 18,050.00
TOTAL			**S/. 20,850.00**

Tabla 49 Egresos Promedio Mensuales antes de la implementación del Sistema Piloto

b. Egresos mensuales después de la implementación del sistema piloto.

Descripción	Cantidad	Costo Unidad	Costo Total
Número promedio de visitas a sitio por mes en Lima	9	S/. 200.00	S/. 1,800.00
Número promedio de visitas a sitio por mes en Provincia	11	S/. 950.00	S/. 10,450.00
TOTAL			**S/. 12,250.00**

Tabla 50 Egresos Promedio Mensuales después de la implementación del Sistema Piloto

7.2.3 Retorno de la Inversión.

A continuación se calcula el ahorro mensual que se logró con la implementación del sistema comparando los egresos antes y después de la implementación del sistema piloto.

Descripción	Monto
Egresos mensuales antes de la implementación del sistema piloto	S/. 20,850.00
Egresos mensuales después de la implementación del sistema piloto	S/. 12,250.00
AHORRO MENSUAL	**S/. 8,600.00**

Tabla 51 Ahorro Mensual

Después de la comparación se logra un ahorro estimado de **S/. 8,600.00** nuevos soles, con lo que se tendría un rápido **retorno de la inversión** calculado para un promedio de **3 meses** logrando así que el proyecto sea económicamente rentable.

CAPÍTULO VIII

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Se concluye que al implementar un sistema de monitoreo y gestión, mediante el uso de VPNs, se optimiza el servicio de soporte en los sistemas de video vigilancia implementados por la empresa Netkrom Technologies.

Se recopiló y analizó la información de las redes a gestionar como el número de elementos que lo conforman y los problemas que usualmente presentan.

Se estableció un canal seguro para el envío de la información de los enlaces vía VPN haciendo uso del protocolo PPTP. El sistema de VPN fueron configuradas en los equipamientos Mikrotik satisfactoriamente, permitiéndonos la interconexión de todas los clientes hacia la sede de la empresa.

Se implementó un centro de datos en el área de soporte de la empresa Netkrom Technologies donde se concentró toda la información en un servidor HP, en el cuál se instaló un sistema propietario gratuito (The Dude) teniendo en cuenta la compatibilidad con el hardware y la familiaridad del usuario con esta marca, para gestionar y monitorear los enlaces implementados por medio del protocolo SNMP.

El sistema de gestión y monitoreo nos permite contar con un historia de eventos, lo cual sirve al administrador para tomar las medidas respectivas en los mantenimientos preventivos.

El sistema de gestión y monitoreo además nos permite la creación de notificaciones, lo cual facilita la visualización de un problema.

El sistema de gestión y monitoreo permite el acceso directo a la interfaz web de los dispositivos, logrando así la configuración remota de los mismos.

El sistema de gestión y monitoreo permite el envío de notificaciones vía email, con ello asegurando una mejor administración del sistema.

Se concluye que al implementar un sistema de monitoreo y gestión se logra optimizar los recursos humanos empleados en la atención de problemas para la reducción de costos y mejorar los tiempos de Respuesta ante averías

Recomendaciones

El servidor donde se instala el sistema de monitoreo debe permanecer encendido y el programa the Dude en ejecución, caso contrario no se recibirán las notificaciones.

Al activar el protocolo SNMP es mejor crear su propia comunidad para proteger la información.

Por medidas de seguridad es importante que las credenciales de acceso a la VPN y al Sistema del Programa The Dude sean de uso restringido.

Es importante que los usuarios tengan credenciales con niveles de administración dependiendo a la función que realizan.

BIBLIOGRAFIA

[1] Gestión de Red- Antoni Barba Martí- Edición UCP 1999

[2] Gestión de Red- Paco Orozco- 2010
https://eetac.upc.edu/ca/fitxers/Gestion_de_red.pdf

[3] Gestión de Redes- Antonio Martín Montes, Carlos León de Mora - 2002

[4] Modelo de Gestión de Red, Grupo SSI
http://gssi.det.uvigo.es/users/mramos/public_html/gprsi/gprsi3.pdf

[5] RFC1157 Simple Network Management Protocol (SNMP)

[6] RFC1156 Management Information Base (MIB)

[7] RFC1155 Structure and Identification of Management Information (SMI)

[8] Fundamentos de Telemática - Jorge Lázaro Laporta, Marcel Miralles Aguiñiga - Edición Uni. Politécnica Valencia 2005

[9] Estudio Científico de las redes de Ordenadores - Ángel Cobo Yera - Edición Visión Libros 2009

[10] Herramientas para circuitos y redes virtuales: interconectividad global segura - Sergio Gonzalo San José

http://pitagoras.usach.cl/~eflores/Icc/cd_redes/REDVIRTUAL.pdf

[11] RFC 2637 Point-to-Point Tunneling Protocol (PPTP)

[12] Introduction to PPTP - Point-to-Point Tunneling Protocol

http://compnetworking.about.com/od/vpn/l/aa030103a.htm

[13] RFC 2784 Generic Routing Encapsulation (GRE)

[14] Window Security-Comparing VPN Options

http://www.windowsecurity.com/articles-tutorials/firewalls_and_VPN/VPN-Options.html

[15] ISA Server 2000 proxy y firewall: optimizar el acceso a internet y la seguridad de la red de la empresa - Philippe Mathon - Ediciones ENI 2002

[16] Configuración de The DUDE como Network Managment System

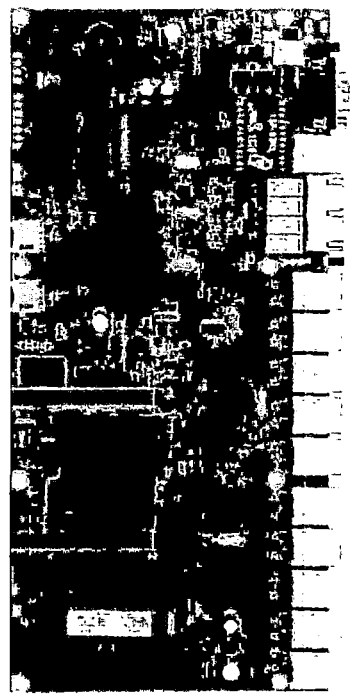
http://www.ryohnosuke.com/foros/index.php?threads/9528/

[17] Manual: The Dude

http://wiki.mikrotik.com

ANEXOS

A. Datasheet de Los Dispositivos.



RB1100AHx2

This device is our best performance 1U rackmount Gigabit Ethernet router. With a dual core CPU, it can reach up to a million packets per second.

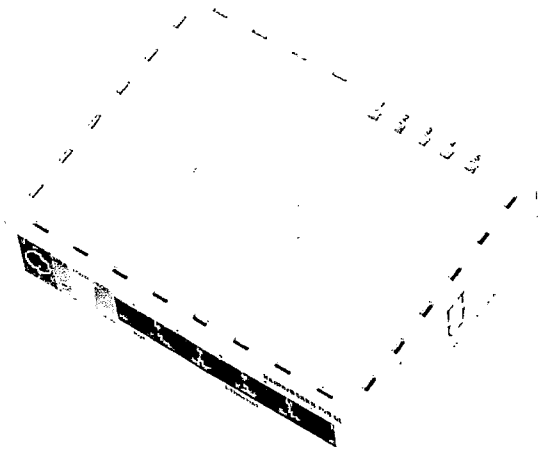
It has thirteen individual gigabit Ethernet ports, two 5-port switch groups, and includes Ethernet bypass capability.

2GB of SODIMM RAM are included, there is one microSD card slot, a beeper and a serial port.

The RB1100AH comes preinstalled in a 1U aluminium rackmount case, assembled and ready to deploy.

CPU	PowerPC P2020 dual core 1066MHz network CPU with IPsec accelerator
Memory	SODIMM DDR Slot, 2GB installed (RouterOS will use only up to 1.5GB)
Boot loader	RouterBOOT, 16MB Flash chip
Data storage	Onboard NAND memory chip, one microSD card slot
Ethernet	Thirteen 10/100/1000 Mbit/s Gigabit Ethernet with Auto-MDI/X
Ethernet	Includes switch to enable Ethernet bypass mode in two ports
Wireless	None
Serial port	One DB9 RS232C asynchronous serial port
Extras	Reset switch, beeper, voltage and temperature sensors
Power options	Built-in power supply IEC C14 standard connector 110/220V), PoE (12-24V on port 13)
Fan	Built-in fans and Fan headers
Dimensions	1U case 44 x 176 x 442 mm, 1770g. Board only, 365g
Operating System	MikroTik RouterOS Level 6 license

RouterBOARD 750GL



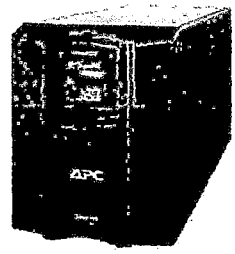
The RB750GL is a small SOHO router in a white plastic case. It has five independent Gigabit Ethernet ports and optional switch chip functionality for wire speed Gigabit throughput.

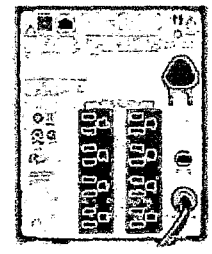
It's probably the most affordable MPLS capable Gigabit router on the market and now it is even more affordable than before. Compared to the previous model, the RB750GL has almost the same performance.

With it's compact design and clean looks, it will fit perfectly into any SOHO environment.

CPU	Atheros AR7242 400MHz network processor
Memory	64MB DDR SDRAM onboard memory
Boot loader	RouterBOOT
Data storage	64MB onboard NAND memory chip
Ethernet	Five 10/100/1000 Mbit/s Gigabit Ethernet ports with Auto-MDI/X, L2MTU frame size up to 4074
Extras	Reset switch
LEDs	5 Ethernet LEDs, power, user (configurable)
Power options	Passive 9-30V PoE, Power Jack 9-30V
Consumption	~6W
Dimensions	113x89x28mm. Weight without packaging and cables: 129g
Operating temperature	-30C to +70C
Operating system	MikroTik RouterOS v5, Level4 license
Package contains	RB750GL, 12V power adapter

APC Smart-UPS C 1000VA LCD 120V
Part Number: SMC1000





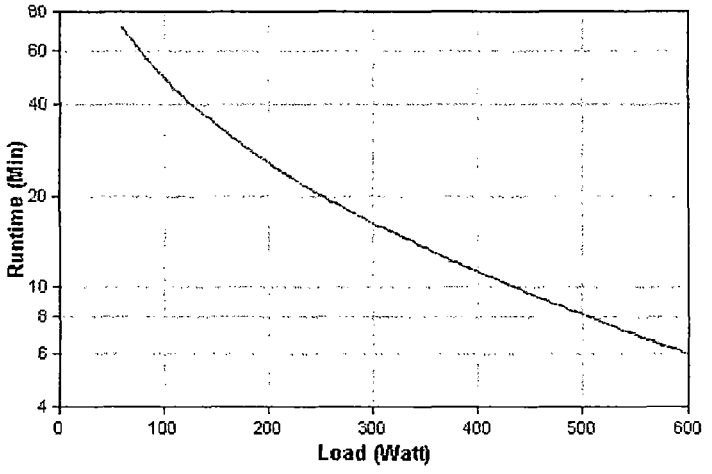
Technical Specifications

Output	
Output Power Capacity	600 Watts / 1000 VA
Max Configurable Power	600 Watts / 1000 VA
Nominal Output Voltage	120V
Output Voltage Distortion	Less than 5%
Output Frequency (sync to mains)	50/60Hz +/- 3 Hz
Topology	Line Interactive
Waveform Type	Sine wave
Output Connections	(8) NEMA 5-15R

Input	
Nominal Input Voltage	120V
Input Frequency	50/60 Hz +/- 3 Hz (auto sensing)
Input Connections	NEMA 5-15P
Cord Length	1.83 meters
Input voltage range for main operations	93 - 130V
Input voltage adjustable range for mains operation	85 - 136V

Batteries & Runtime

Battery Type	Maintenance-free sealed Lead-Acid battery with suspended electrolyte : leakproof
Typical recharge time	3 hour(s)
RBC™ Quantity	1
Runtime Graph	



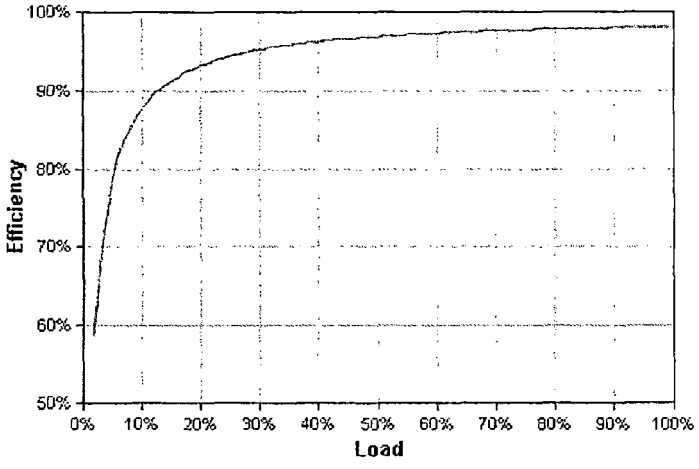
Hover over the line on the graph above to view the runtime at any desired load

Curve fit to measured runtime data. All measurements taken with new, fully charged batteries, at typical environmental conditions, with no electrical input and balanced resistive load (PF = 1.0) output.

View Enlarged Graph View Runtime Chart

Energy Use/Efficiency

Load	Efficiency
25%	94.6%
50%	97.0%
75%	97.8%
100%	98.1%



Hover over the line on the graph above to view the efficiency at any desired load

Curve fit of data measured in accordance with the ENERGY STAR Program Requirements Product Specification for Uninterruptible Power Supplies (UPSs) - Eligibility Criteria Version 1.0. All measurements taken in normal mode(s), at typical environmental conditions, with 120V/60Hz electrical input and balanced resistive load (PF = 1.0) output

Communications & Management

Interface Port(s)	RJ-45 Serial, USB
Control panel	Multi-function LCD status and control console
Audible Alarm	Alarm when on battery : distinctive low battery alarm : configurable delays
Emergency Power Off (EPO)	--

Surge Protection and Filtering

Surge energy rating	455 Joules
Filtering	Full time multi-pole noise filtering : 0.3% IEEE surge let-through : zero clamping response time : meets UL 1449

Physical

Maximum Height	219.00 mm
Maximum Width	171.00 mm
Maximum Depth	439.00 mm
Net Weight	17.27 KG
Shipping Weight	19.55 KG
Shipping Height	376.00 mm
Shipping Width	328.00 mm
Shipping Depth	595.00 mm
Color	Black
Units per Pallet	12.00

Environmental

Operating Environment	0 - 40 °C
Operating Relative Humidity	0 - 95%
Operating Elevation	0-3000 meters
Storage Temperature	-15 - 45 °C
Storage Relative Humidity	0 - 95%
Storage Elevation	0-15000 meters
Audible noise at 1 meter from surface of unit	41.00 dBA
Online Thermal Dissipation	100.00 BTU/hr

Conformance

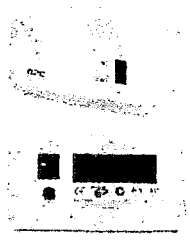
Regulatory Approvals	CSA, ENERGY STAR (USA), NOM, UL 1778
Standard Warranty	2 years repair or replace

Sustainable Offer Status

RoHS	Compliant
REACH	REACH: Contains No SVHCs

**The time to recharge to 90% of full battery capacity following a discharge to shutdown using a load rated for 1/2 the full load rating of the UPS.

Line-R 1200VA Automatic Voltage Regulator



APC Line-R,Input 230V /

Input	
Nominal Input Voltage	230V
Input Frequency	50/60 Hz
Input Connections	IEC-320 C14
Surge Protection and Filtering	
Surge energy rating	300 Joules
Physical	
Maximum Height	116.00 mm
Maximum Width	214.00 mm
Maximum Depth	141.00 mm
Net Weight	4.20 KG
Shipping Weight	4.50 KG
Shipping Height	175.00 mm
Shipping Width	273.00 mm
Shipping Depth	207.00 mm
Master Carton Units	4.00
Master Carton Dimensions (Length x Width x Height)	425.00 mm
Master Carton Weight	19.09 KG
Color	Beige
SCC Codes	10731304197932
Units per Pallet	64.00
Environmental	
Operating Environment	0 - 40 °C
Operating Relative Humidity	5 - 95%
Operating Elevation	0-3000 meters
Storage Temperature	-25 - 65 °C
Storage Relative Humidity	5 - 95%
Storage Elevation	0-15000 meters
Conformance	
Regulatory Approvals	C-tick, CE, EN 55024, EN 60950, GOST, GS Mark
Standard Warranty	2 years repair or replace

LED 42" 42LB5500 LG

Ficha Técnica

Atributos	Detalle
Tecnología	LED
Resolución	Full HD
Tamaño de pantalla	42"
WiFi incorporado	-
Smart TV	No
3D	No
Tipo de 3D	-
Control por voz	-
Control por movimiento	-
HDMI	Si
Tipo	-
Modelo	42LB5500
Color	-
Tasa de refresco	-
Wifi Ready	-
Procesador	-
Sintonizador digital	-
Potencia de parlantes	-
Camara incorporada	-
Aplicaciones destacadas	-
Conexión óptica de audio digital	-
Conexión auxiliar 3.5 mm	-
USB	Si
Conexión RCA	-
Conexión VGA	-
Puerto Ethernet	-
Destacados	-

Lentes 3D incluidos	-
Control remoto	SI
Accesorios incluidos	-
Origen	-
Alto (con s/n base)	-
Profundidad (con/sin base)	-
Ancho	-
Peso (con/sin base)	-
Garantía del producto	2 años
Garantía extendida	No incluida

Centro de Soporte de HP

HP Compaq Pro 6300 Small Form Factor PC - Specifications

Physical specifications

Weights and dimensions (configured with 1 HDD and 1 ODD)

Feature	Description
Chassis (H x W x D)	100 x 338 x 379 mm (4.0 x 13.3 x 14.9 in)
System volume	13.0 L (790.3 cu in)
System weight	7.6 kg (16.7 lb)
Maximum supported weight (desktop orientation)	35.0 kg (77.0 lb)
Tower stand (H x W x D)	29 x 176 x 200 mm (1.1 x 7.0 x 7.9 in)
Packaging (H x W x D)	229 x 500 x 594 mm (9.0 x 19.8 x 23.4 in)
Shipping weight	8.1 kg (17.9 lb)
Palletization profile	• 4-units per layer • 10-layer maximum • 40-units per pallet

Graphics specifications

Intel HD graphics

Feature	Description
VGA controller	Integrated
DisplayPort	• 1.1a • Integrated, multimode capable • supports HDCP and audio over DisplayPort
Bus type	PCI Express x16
RAMDAC	• Integrated • 350 MHz
Maximum graphics memory	**Microsoft Windows XP:** Up to 1GB **Microsoft Windows 7:** Up to 1.7GB
HW video decode	AVC/VC1/MPEG2/JPEG/MJPEG/PAVP
Maximum color depth	32 bits/pixel
Supported display resolutions and refresh rates [1]	

Resolution	Analog	Digital
640 x 480	85	60
800 x 600	85	60
1024 x 768	85	60
1280 x 720	85	60
1280 x 1024	85	60
1440 x 900	75	60
1600 x 1200	85	60
1680 x 1050	75	60
1920 x 1080	85	60-R
1920 x 1200	85	60-R
1920 x 1440	85	N/A
2048 x 1536	75	N/A
2560 x 1600	N/A	60[2]

AMD Radeon HD 6350 Graphics Card

Feature	Description
Form factor	• PCI Express x16 (generation 2.0) • Low Profile, half length, 2.3 in x 6.6 in • Full height bracket utilized when configured to MT
Graphics controller	AMD HD 6350 GPU
Output connector	• Single DMS-59 connector • Supports dual analog displays with included DMS-59 to dual VGA Y cable. • Also supports dual digital displays with an optional DMS-59 to dual DVI cable.
Core clock	650 MHz
Memory clock	800 MHz
Memory frame buffer	512MB, DDR3, 64-bit wide
Bus type	• PCI Express x16 • Generation 2.0
Maximum vertical refresh	85 Hz
Display support	Integrated 400 MHz RAMDAC
Display maximum resolution	• Digital 1900 x 1200 • Analog 2048 x 1536
Maximum power consumption	19.9 W
Supported graphics APIs	• HDCP supported on DVI output using optional DMS-59 to dual DVI cable. • DirectX 11 support in hardware. • OpenGL 4.0 support in hardware.
Supported display resolutions and refresh rates [1]	

Resolution	Analog	Digital
640 x 480	85	60
800 x 600	85	60
1024 x 768	85	60
1280 x 720	85	60
1280 x 1024	85	60
1440 x 900	75	60
1600 x 1200	85	60
1680 x 1050	75	60
1920 x 1080	85	60-R
1920 x 1200	85	60-R
1920 x 1440	85	N/A
2048 x 1536	75	N/A
2560 x 1600	N/A	N/A

AMD Radeon HD 7450 Graphics Card

Feature	Description
Form factor	• PCI Express x16 (generation 2.0) • Low Profile, half length, 6.57 x 14.48 cm (2.586 x 5.7 in) • Full height bracket utilized when configured to MT
Graphics controller	Nvidia GT218 GPU
Output connector	• Single DMS-59 connector • Supports dual analog displays with included DMS-59 to dual VGA Y cable. • Support dual digital displays with an optional adapter.
RAMDAC	Dual 400 MHz
Core clock	520 MHz
Memory clock	790 MHz
Memory frame buffer	512MB DDR3, 64-bit wide
Bus type	• PCI Express x16 • Generation 2.0
Maximum vertical refresh	85 Hz
Display support	Integrated 400 MHz RAMDAC
Display maximum resolution	• Digital 1900 x 1200 • Analog 2048 x 1536
Maximum power consumption	19.9 W
Supported graphics APIs	• DirectX 11 support in hardware. • OpenGL 4.0 support in hardware.
Supported display resolutions and refresh rates [1]	

Resolution	Analog	Digital
640 x 480	85	60
800 x 600	85	60
1024 x 768	85	60
1280 x 720	85	60
1280 x 1024	85	60
1440 x 900	75	60
1600 x 1200	85	60
1680 x 1050	75	60
1920 x 1080	85	60-R
1920 x 1200	85	60-R
1920 x 1440	85	60[2]
2048 x 1536	75	60[2]
2560 x 1600	N/A	60[3]

NVIDIA NVS 300 Graphics Card

Feature	Description
Form factor	• PCI Express x16 (generation 2.0) • Low Profile, half length, 2.3 x 6.6 in • Full height bracket utilized when configured to MT
Graphics controller	AMD HD 7450 GPU (based on AMD Radeon HD 6000 series technology)
Output connector	Dual-link (DL) DVI-I and DisplayPort output ports
Core clock	625 MHz
Memory clock	800 MHz
Memory frame buffer	1GB, DDR3, 64-bit wide
Maximum pixel clock (analog)	400 MHz
Overlay planes	One 16-bit video overlay plane
Video acceleration	• Directx 10.1 • OpenGL 3.3 • CUDA • DirectCompute
Supported Graphics APIs	• OpenGL 3.3 support in hardware • DirectX 10.0 support in hardware
High-definition Video Processor (HDVP)	• Inbuilt video decoder for multiple video formats including MPEG2, VC-1, WMV9, H.264, and MVC • Capable of decoding dual Video Streams at HD (1080p) resolutions • Hardware color-space conversion (YUV 4:2:2 and 4:2:0) • High-Quality in-built Filtering/Scaling • Stereo & HD Audio (LPCM 7.1) support for HDMI outputs (HDMI via optional DVI-HDMI dongles) with the DMS-59 to DisplayPort Adapter
Supported display resolutions and refresh rates [1]	

Resolution	Analog	Digital
640 x 480	85	60
800 x 600	85	60
1024 x 768	85	60
1280 x 720	85	60
1280 x 1024	85	60
1440 x 900	75	60
1600 x 1200	85	60
1680 x 1050	75	60
1920 x 1080	85	60-R
1920 x 1200	85	60-R
1920 x 1440	85	60[2]
2048 x 1536	75	60[2]
2560 x 1600	N/A	60[3]

NVIDIA NVS 310 Graphics Card

Feature	Description
Bus type	PCI Express x16
Graphics chip	GT218
Core clock	589 MHz

Memory clock	790 MHz
Frame buffer	512MH DDR2, 64-bit wide
Audio support	• Audio supported through DisplayPort only • Integrated HD audio codec supports linear PCM and Dolby Digital (7.1) audio formats
Maximum power	25 W
Dimensions	68.90 x 167.65 mm (2.71 x 6.6 in)
Maximum vertical refresh rate	85 Hz
Display support	Integrated 400 MHz RAMDAC
Display maximum resolution	• Digital 2560 x 1600 • Analog 2048 x 1536
Board display options	Supports two displays via dual DisplayPort connectors
Supported display resolutions and refresh rates [1]	

Resolution	Analog	Digital
640 x 480	85	60
800 x 600	85	60
1024 x 768	85	60
1280 x 720	85	60
1280 x 1024	85	60
1440 x 900	75	60
1600 x 1200	85	60
1680 x 1050	75	60
1920 x 1080	85	60-R
1920 x 1200	85	60-R
1920 x 1440	85	NA
2048 x 1536	75	NA
2560 x 1600	N/A	60[2]

Hard disk and solid state storage specifications

Storage drive support

Feature	ASR	QTO	MSO
Number of supported devices	1	1	2
Drive position	1	2	1,3

Controller

Feature	Description
Hard drive controller	These systems provide four serial ATA (SATA) interfaces that support transfer rates up to 6.0 Gb/s (for ports 0 and 1, 3 Gb/s on all others). These systems can also support an external SATA (eSATA) device through an optional bracket/cable assembly.
SATA interfaces	• 2 ea. SATA 3.0 • 1 ea. SATA 2.0 • 1 ea. eSATA
Host SATA controller	Advanced Host Controller Interface (AHCI) Revision 1.2. The specification includes a description of the hardware/software interface between system software and the host controller hardware.

HP 250-GB 7200rpm SATA 6.0 Gb/s 3.5 in Hard Disk Drive

Feature	Description
Capacity	250,059,350,016 bytes
Rotational speed	7,200 rpm
Interface	Serial ATA 3.0 (6.0 Gb/s)
Buffer size	8MB
Logical blocks	488,397,168
Seek time (typical reads, includes controller overhead, including settling)	• Single track: 1.0 ms • Average: 8.5 ms • Full-stroke: 18 ms
Height (nominal)	2.54 cm (1 in)
Width (nominal)	• Media diameter: 8.89 cm (3.5 in) • Physical size: 10.2 cm (4 in)
Operating temperature	5° to 55°C (41° to 131°F)

HP 500-GB 7.2K rpm SATA 6.0 Gb/s 3.5 in Hard Disk Drive

Feature	Description
Capacity	500,107,862,016 bytes
Rotational speed	7,200 rpm
Interface	Serial ATA 3.0 (6.0 Gb/s)
Buffer size	16MB
Logical blocks	976,773,168

Seek time (typical reads, includes controller overhead, including settling)	• Single track: 2.0 ms • Average: 11 ms • Full-stroke: 21 ms
Height (nominal)	2.54 cm (1 in)
Width (nominal)	• Media diameter: 8.89 cm (3.5 in) • Physical size: 10.2 cm (4 in)
Operating temperature	5° to 55°C (41° to 131°F)

HP 1-TB 7.2K rpm SATA 6.0 Gb/s 3.5 in Hard Disk Drive

Feature	Description
Capacity	1,000,204,886,016 bytes
Rotational speed	7,200 rpm
Interface	Serial ATA 3.0 (6.0 Gb/s)
Buffer size	32MB
Logical blocks	1,953,525,168
Seek time (typical reads, includes controller overhead, including settling)	• Single track: 2.0 ms • Average: 11 ms • Full-stroke: 21 ms
Height (nominal)	2.54 cm (1 in)
Width (nominal)	• Media diameter: 8.89 cm (3.5 in) • Physical size: 10.2 cm (4 in)
Operating temperature	5° to 55°C (41° to 131°F)

HP 120-GB Solid State Drive

Feature	Description
Unformatted capacity	120GB
Architecture	Multi Level Cell (MLC) NAND Flash with wear leveling 10 channel controller
Interface	Serial ATA 2.0 (3.0 Gb/s)
Dimensions (W x H x D)	6.98 x 0.95 x 10.2 cm (2.74 x 0.37 x 4 in)
Weight	80 g (0.18 lb)
Bandwidth performance	• Sustained sequential read: Up to 250 MB/s • Sustained sequential write: Up to 70 MB/s • Random read: Up to 35K IOPs • Random write: Up to 6.6K IOPs
Latency	• Read: 65 ms • Write: 85 ms
Power	• DC power requirement: 5 V dc 5%-100 mV ripple p-p • Total power consumption: 0.15 W (active); 0.075 W (idle)
Useful drive life	• 35TB written • up to 20 GB/day for 5 years
Environmental (all conditions, non-condensing)	**Operating temperature:** 0° to 70°C (32° to 158°F) **Relative humidity:** 5% to 95% **Maximum wet bulb temperature (operating):** 29°C (84°F) **Shock:** 1,500G/1.0 ms

HP 128 GB Solid State Drive (SSD)

Feature	Description
Unformatted capacity	128GB[1]
Architecture	Multi Level Cell (MLC) NAND
Interface	SATA 6 GB/sec
Dimensions (W x H x D)	6.985 x 0.7 x 10.05 cm (2.75 x 0.276 x 3.96 in)
Weight	73 g (0.16 lb)
Bandwidth performance	• Sustained sequential read: Up to 450 MB/s • Sustained sequential write: Up to 260 MB/s • Random read: Up to 46K IOPs • Random write: Up to 56K IOPs
Latency	• Read: 55µs (TYP) • Write: 55µs (TYP)
Power	**DC power requirement:** • Min 4.5 V • Max 5.5 V **Total power consumption:** • 160 mW (Active) • <85 mW 85 mW (Idle)
Useful drive life	1.2 million device hours[2]
Environmental (all conditions, non-condensing)	**Operating temperature:** 0° to 70°C (32° to 158°F)

	Relative humidity: 5% to 95% **Maximum wet bulb temperature (operating):** 29°C (84°F) **Shock:** 1,500G/0.5 ms
Regulations	• UL • CSA • EN 60950-2000 • CISPR Pub 22 Class B • CNS 13438 • AS/NZS CISPR 22:2002 Class B • Korea KCC • CE Mark
Option kit contents	• HP 128GB Solid State Drive (SSD) • Documentation • 3.5-inch bay adapter bracket • 3.5-inch bay adapter bracket screws • SATA cable

Removable storage specifications

HP Blu-ray writer drive

Feature	Description
AMO part number	AR482AA
Height	• 5.25-inch • Half-height • Tray-load
Orientation	Either horizontal or vertical
Interface type	SATA
Disc capacity	50GB DL or 25GB standard
Dimensions (W x H x D)	15.0 x 4.4 x 19.0 cm (5.9 x 1.7 x 8.0 in)
Weight (max)	907 g (2.0 lb)
Disc capacity	**DVD-ROM:** 8.5GB DL or 4.7GB standard **Blu-ray:** 50GB DL or 25GB standard **Full stroke DVD:** <250 ms (seek) **Full stroke CD:** <210 ms (seek) **Blu-ray:** <275 ms (seek) **Startup time (Time to drive ready from tray loading):** • BD-ROM (SL/DL) 25S/28S • BD-R (SL/DL) 25S/28S • BD-RE (SL/DL) 25S/28S • DVD-ROM (SL/DL) 18S/18S • DVD-R (SL/DL) 25S/25S • DVD-RW 25S • DVD+R (SL/DL) 25S/25S • DVD+RW DVD+RW 25S • DVD-RAM 45S • CD-ROM 15S
Maximum data transfer rates	**CD-ROM read:** • CD-ROM up to 40X • CD-R up to 40X • CD-RW up to 40X **DVD-ROM read:** • DVD-RAM up to 5X • DVD+RW up to 10X • DVD-RW up to 10X • DVD+R DL up to 8X • DVD-R DL up to 8X • DVD-ROM up to 16X • DVD-ROM DL up to 8X • DVD+R up to 12X • DVD-R up to 12X **Blu-ray:** • BD-ROM up to 6X • BD-ROM DL up to 4.8X • BD-R up to 6X • BD-R DL up to 4.8X • BD-R up to 6X • BD-RE SL/DL up to 4.8X
Power	**Source:** SATA DC power receptacle **DC power requirement:** • 5 V dc ± 5%-100 mV ripple p-p

	• 12 V dc ± 5%-200 mV ripple p-p **DC current:** • 5 V dc -1000 mA typical • 1600 mA maximum 12 V dc -600 mA typical • 1400 mA maximum
Environmental (all conditions non-condensing)	**Temperature (operating):** 5° to 50°C (41° to 122°F) **Relative humidity (operating):** 10% to 90% **Maximum wet bulb temperature (operating):** 30°C (86°F)

HP SuperMulti DVD writer drive

Features	Description
AMO part number	AR630AT
Height	• 5.25-inch • Half-height • Tray-load
Orientation	Either horizontal or vertical
Interface type	Serial ATA
Dimensions (W x H x D)	15.0 x 4.4 x 20.3 cm (5.9 x 1.7 x 8.0 in)
Weight (max)	1.2 kg (2.6 lb)
Performance	**CD Media Read Access:** • Random: <120 ms typical • Full stroke: <200 ms typical **DVD Media Read Access:** • Random: <120 ms typical • Full stroke: <200 ms typical **CD Media Read Transfer:** • Digital Audio Extraction (CD-ROM, CD-R): Up to 6000 KB/s (40X) • Digital Audio Extraction (CD-RW): Up to 4800 KB/s (32X) Video CD Playback Up to 2400 KB/s (16X) **DVD Media Read Transfer:** • DVD-ROM SL Read: Up to 21600 KB/s (16X) • DVD-ROM DL Read: Up to 10800 KB/s (8X) • DVD Video Playback: Up to 10800 KB/s (8X) • DVD Video SL (other than playback): Up to 21600 KB/s (16X) • DVD Video DL (other than playback): Up to 10800 KB/s (8X) • DVD-R: Up to 21600 KB/s (16X) • DVD+R: Up to 21600 KB/s (16X) • DVD-RW: Up to 10800 KB/s (8X) • DVD-R DL: Up to 10800 KB/s (8X) • DVD+RW: Up to 10800 KB/s (8X) **CD Media Write Transfer:** • CD-R Write: Up to 6000 KB/s (40X) • CD-RW: 600 KB/s (4X) • CD-RW (High speed): 1500 KB/s (10X) • CD-RW (Ultra speed): Up to 3600 KB/s (24X) • CD-RW (Ultra speed+): Up to 4800 KB/s (32X) **DVD Media Write Transfer:** • DVD+R: Up to 21600 KB/s (16X) • DVD+R DL (v1.2): Up to 16200 KB/s (12X) • DVD+R DL (v1.1): Up to 10800 KB/s (8X) • DVD+RW (Volume 2 v1.0): Up to 10800 KB/s (8X) • DVD+RW (Volume 1 v1.3): Up to 5400 KB/s (4X) • DVD-R (v2.1 rev. 6.0): Up to 16200 KB/s (12X) • DVD-R (v2.1 rev. 4.0): Up to 21600 KB/s (16X) • DVD-R DL (v3.0 rev. 5.0): Up to 10800 KB/s (8X) • DVD-R DL (v3.0 rev. 3.0): Up to 10800 KB/s (8X) • DVD-RW (v1.2 rev. 3.0) 8100 KB/s (6X) • DVD-RW (v1.2 rev. 2.0): Up to 5400 KB/s (4X) • DVD-RAM (v2.2 rev. 5.0): Up to 16200 KB/s (12X) • DVD-RAM (v2.2 rev. 2.0): Up to 6750 KB/s (5X)
Media compatibility	

Media	Read	Write
CD-ROM	Yes	No
CD-R	Yes	No
CD-RW	Yes	No
DVD-ROM	Yes	No
DVD-ROM DL	Yes	No
DVD-RAM	Yes	No
DVD+R	Yes	No
DVD+R DL	Yes	No
DVD+RW	Yes	No
DVD-R	Yes	No
DVD-RW	Yes	No
DVD-R DL	Yes	No

Power supply			
	DC power requirement	5 V dc ± 5%	100 mV ripple p-p
		12 V dc ± 5%	200 mV ripple p-p
	DC Current	5 V dc	<1000 mA (typical) 1600 mA (max.)
		12 V dc	1200 mA (typical) 2000 mA (max.)
Rear panel	• SATA Power Connector, 15-pin • SATA Data Connector, 7-pin • Markings to identify each connector		
Environmental conditions (all conditions non-condensing)	**Operating temperature:** 5° to 50°C (41° to 122°F) **Storage temperature:** -30°C to 60°C (-22°F to 140°F) **Relative humidity:** 10% to 90% **Maximum wet bulb temperature:** 30°C (86°F) **Altitude:** 0 to 3,100 meters (0 to 10,171 ft.)		

HP DVD-ROM drive

AMO part number	AR629AA
Height	• 5.25-inch • Half-height • Tray-load
Orientation	Either horizontal or vertical
Interface type	Serial ATA
Dimensions (W x H x D)	14.8 x 4.2 x 17.5 cm (5.8 x 1.7 x 6.9 in)
Weight (max)	950 kg (2.1 lb)
Performance	**CD Media Read Access:** • Random: <120 ms typical • Full stroke: <200 ms typical **DVD Media Read Access:** • Random: <130 ms typical • Full stroke: <240 ms typical **CD Media Read Transfer:** • Digital Audio Extraction (CD-ROM, CD-R): Up to 6000 KB/s (40X) • Digital Audio Extraction (CD-RW): Up to 4800 KB/s (32X) Video CD Playback Up to 2400 KB/s (16X) • Digital Audio Extraction (CD-RW): Up to 4800 KB/s (32X) **DVD Media Read Transfer:** • Video CD Playback: Up to 2400 KB/s (16X) • DVD-ROM SL Read: Up to 21600 KB/s (16X) • DVD-ROM DL Read: Up to 10800 KB/s (8X) • DVD Video Playback: Up to 10800 KB/s (8X) • DVD Video SL (other than playback): Up to 21600 KB/s (16X) • DVD Video DL (other than playback): Up to 10800 KB/s (8X) • DVD-R: Up to 21600 KB/s (16X) • DVD+R: Up to 21600 KB/s (16X) • DVD-RW: Up to 10800 KB/s (8X) • DVD-R DL: Up to 10800 KB/s (8X) • DVD+RW: Up to 10800 KB/s (8X)

Media compatibility			
	CD-ROM	Yes	No
	CD-R	Yes	No
	CD-RW	Yes	No
	DVD-ROM	Yes	No
	DVD-ROM DL	Yes	No
	DVD-RAM	Yes	No
	DVD+R	Yes	No
	DVD+R DL	Yes	No
	DVD+RW	Yes	No
	DVD-R	Yes	No
	DVD-RW	Yes	No
	DVD-R DL	Yes	No

Power supply			
	DC power requirement	5 V dc ± 5%	100 mV ripple p-p
		12 V dc ± 5%	200 mV ripple p-p
	DC Current	5 V dc	1000 mA (typical) 1600 mA (max.)
		12 V dc	1200 mA (typical) 2000 mA (max.)
		Total Drive Power (Standby Mode)	<2.5 W

Rear panel	• SATA Power Connector, 15-pin • SATA Data Connector, 7-pin • Markings to identify each connector
Environmental conditions (all conditions non-condensing)	**Operating temperature:** 5° to 50°C (41° to 122°F) **Storage temperature:** -30°C to 60°C (-22°F to 140°F) **Relative humidity:** 10% to 90% **Maximum wet bulb temperature:** 30°C (86°F) **Altitude:** 0 to 3,100 meters (0 to 10,171 fL)

HP 22-n-1 Media Card Reader

Feature	Description
USB interface	USB 2.0 High-speed interface[1]
Advance protocol support	• Supports hardware ECC (Error Correction Code) function • Supports hardware CRC (Cyclic Redundancy Check) function • Supports MS 4-bit parallel transfer mode • Supports MS-PRO 4-bit parallel transfer mode • Supports MS PRO-HG Duo 4-bit parallel transfer mode • Supports SD 4-bit parallel transfer mode • Supports high-speed 50 Mhz SD 4-bit card (version 2.0) • Supports high-speed 52 Mhz MMC 8-bit card (version 4.2) • Supports CF v4.0 with PIO mode 6 and Ultra DMA mode
Supported media type	• CompactFlash Type I • CompactFlash Type II • Microdrive MultiMediaCard (MMC) • Reduced Size MultiMediaCard (RS MMC) • MultiMediaCard 4.2 (MMC Plus, including MMC Plus HC) • Reduced Size MultiMediaCard 4.2 (MMC Mobile, including MMC Mobile HC) • Secure Digital Card (SD) • Secure Digital High Capacity (SDHC) • miniSD • miniSD High Capacity • Micro SD (T-Flash) • Micro SD HC • Memory Stick • Memory Stick Select • Memory Stick Duo (MS Duo) • Memory Stick PRO (MS PRO) • Memory Stick PRO Duo (MS PRO Duo) • Memory Stick PRO-HG Duo • MagicGate Memory Stick (MG) • MagicGate Memory Stick Duo • xD-Picture Card
Supported media type with card adapter	• Memory Stick Micro (M2) • MMC Micro
Environmental	**Operational environmental extremes:** Test parameters/conditions - Power applied, unit operating on system ±5% nominal supply voltage. • 10°C 10% R.H. <= 24 hours • 10°C 90% R.H. <= 24 hours • 20°C 90% R.H. <= 24 hours • 30°C 90% R.H. <= 24 hours • 40°C 90% R.H. <= 24 hours • 50°C 90% R.H. <= 24 hours • 50°C 10% R.H. <= 24 hours **Storage environmental extremes** Test parameters/conditions: • 60°C (140°F) @ 80% R.H. for 96 hours • -30°C (-22°F) @ 20% R.H. for 48 hours • No power applied • Delta °C <1.0°C/min • Delta % R.H. <1.5% R.H./min
Approvals	• USB-IF • WHQL • Compliant with USB Mass Storage Class Bulk only Transport Specification Rev. 1.0 • Compliant Intel Front Panel I/O Connectivity Design Guide V. 1.3 • FCC • CE • BSMI • C-Tick • VCCI • MIC • cUL • TUV-T

Power specifications

Features	Description
Standard efficiency	240 W active PFC
High efficiency [1]	240 W active PFC 87/90/87% efficient @ 20/50/100% load
Operating voltage range	90 - 264 V ac
Rated voltage range	100 - 240 V ac
Rated line frequency	50/60 Hz
Operating line frequency range	47 - 63 Hz
Rated input current	4A
Rated input current with energy efficient [1] power supply	4A
Current leakage (NFPA 99)	<275 µA
Power supply fan	92 mm variable speed
Power cord length	1.83 m (6.0 ft.)

Memory specifications

Slot 1 is black and must always be populated. Not all memory configurations possible are represented below:

Memory configurations

Total Memory	Socket			
	Channel A		Channel B	
	1 (black)	2 (white)	3 (white)	4 (white)
2GB	2GB	unpopulated	unpopulated	unpopulated
4GB (dual channel)	2GB	unpopulated	2GB	unpopulated
8GB (dual channel)	2GB	2GB	2GB	2GB
16GB (dual channel)	8GB	4GB	4GB	4GB

Network specifications

Intel 82579LM GbE Network Connection (integrated)

Features	Description
Connector	RJ-45
System interface	Integrated on PCA
Controller	Intel 82579LM GbE platform LAN connect networking controller
Memory	24KB FIFO packet buffer memory
Data rates supported	10/100/1000 Mb/s
IEEE compliance	• 802.1P • 802.1Q • 802.2 • 802.3 • 802.3ab • 802.3az • 802.3u
Bus architecture	PCI Express and SMBus
Data transfer mode	PCIe-based interface for active state operation (S0 state) and SMBus for host and management traffic (Sx low power state)
Power requirement	Requires 3.3 V and 1.05 V or just 3.3 V with integrated regulators Power consumption 0.697 W
Boot ROM support	Yes
Network transfer mode	• Full-duplex • Half-duplex (not supported for the 1000BASE-T transceiver)
Network transfer rate	• 10BASE-T (half-duplex) 10 Mb/s • 10BASE-T (full-duplex) 20 Mb/s • 100BASE-TX (half-duplex) 100 Mb/s • 100BASE-TX (full-duplex) 200 Mb/s • 1000BASE-T (full-duplex) 2000 Mb/s
Environmental	**Operating temperature:** 0° to 85°C **Operating Humidity:** 60% RH
Management	• WOL • auto MDI crossover • PXE • Muti-port teaming • RSS • Advanced cable diagnostic.

Alerting	• ASF 2.0 support • AMT 7.0 support

Intel Gigabit CT Desktop Network Interface Controller

Feature	Description
Connector	RJ-45
System interface	PCI Express x1
Controller	Intel WG82574L Gigabit Ethernet Controller
Memory	Integrated Dual 48K configurable transmit receive FIFO Buffers
Data rates supported	10/100/1000 Mb/s
IEEE compliance	• 802.1P • 802.1Q • 802.2 • 802.3 • 802.3AB and 802.3u compliant • 802.3x flow control
Bus architecture	PCI-E 1.0a
Data path width	• X1 • 250 MB/s • Bi-directional interface
Data transfer mode	Bus-master DMA
Hardware certifications	• FCC • B • CE • TUV- cTUVus Mark Canada and United States • TUV- GS Mark for European Union
Power requirement	Aux 3.3 V, 3.0 W in 1000base-T and 2.0 W in 100Base-T
Boot ROM support	Yes
Network transfer rate	• 10BASE-T (half-duplex) 10 Mb/s • 10BASE-T (full-duplex) 20 Mb/s • 100BASE-TX (half-duplex) 100 Mb/s • 100BASE-TX (full-duplex) 200 Mb/s • 1000BASE-T (full-duplex) 2000 Mb/s (actual rate limited by PCI Bus)
Environmental	**Operating temperature:** 0° to 55°C (32° to 131°F) **Operating humidity:** 85% at 55°C (131°F)
Management	• WOL • PXE • DMI • WFM 2.0
Dimensions	12.1 x 5.7 x 2.0 cm (4.75 x 2.25 x 0.8 in)

Feature	Description
Dimensions (L x H)	7.0 x 5.7 cm (2.8 x 2.2 in)
Weight	40 g (0.08 lbs)
Controller	Ralink RT2790
System interface	PCI Express x1
Network standard	802.11 b/g/n
Frequency band	2.400 - 2.497 GHz
Operating temperature	-10° to 65°C, operating (14° to 149°F, operating)
Storage temperature	-40° to 80°C, non-operating (-40° to 176°F, non-operating)
Humidity	• 10 - 90% operating • 5 - 95% non-operating
Operating voltage	• 3.3 V +/- 9% • 12 V +/- 8%
Power consumption	<table><tr><th>Platform/Power Mode</th><th>Power Consumption</th></tr><tr><td>Maximum Power Consumption</td><td>10 W</td></tr><tr><td>Transmit Only</td><td>4 W maximum averaged power over 1 second</td></tr><tr><td>Transmit Packet or Active Scanning</td><td>1000 mA peak current for 100 ms or longer</td></tr><tr><td>Receive Only Mode or Idle without IEEE PSP mode enabled</td><td>3 W maximum averaged over 1 second</td></tr><tr><td>Idle, with IEEE PSP mode enabled</td><td>1.0 W maximum averaged over 1 second</td></tr><tr><td>Transmit Disabled (turned off in software)</td><td>50 mW maximum, averaged over 1 secon</td></tr><tr><td>Platform in S3 or S4 (power removed from Low Profile PCI Express Card)</td><td>5 mW maximum, averaged over 1 second</td></tr></table>
Output power (approximate)	**802.11b mode:** +19 dBm +/- 1.0 dB maximum **802.11g mode:** +17 dBm +/- 1.0 dB maximum **EWC mode:** +17 dBm +/- 1.0 dB maximum (total power in all transmit chains)
Security	• IEEE and WiFi compliant 64/128 bit WEP encryption • AES: CCM

	• 802.1x authentication • WPA: 802.1x, WPA-PSK and TKIP • WPA2 certification • IEEE 802.11i Cisco Certified Extensions, all versions through V5
Antenna	HP part number 497317-003
Certifications	Wi-Fi certified
Certifications for use by country	• United States • Canada • Peru • Taiwan

Audio specifications

High definition audio

Feature	Description
Type	Integrated
HD Stereo codec	Realtek 2-channel ALC221 codec
Audio I/O ports	• Front microphone-In (150-K ohm Input Impedance) • Rear Line-In/Microphone input (150-K ohm Input Impedance, function is configurable by audio driver) • Rear Line-Out* (190 ohms Output Impedance, expects at least a 10-K ohm load) • Front Headphone-Out (0.5 Ohm Output Impedance, expects at least a 32 ohm load) • Front Microphone/Headphone jack is re-task able to provide Microphone input, line-in or • Headphone output to support connecting two headphones to the front of the system. When configured as a second front headphone output, both front headphone outputs are always driven with the same signal. • All ports are 3.5 mm
Internal speaker amplifier	• 1.5 W amplifier for the internal speaker only. • External speakers must be powered externally. • Rear Line-in audio port is re-taskable as either Line-in or Microphone-In.
Multi-streaming capable	Multi-streaming can be enabled in the Realtek control panel to allow independent audio streams to be sent to/from the front and rear jacks.
Sampling	8 kHz - 192 kHz
Wavetable syntheses	Yes - Uses OS soft wavetable
Analog audio	Yes
Number of Channels on Line-Out	Stereo (Left & Right channels)
Internal speaker	Yes
External speaker jack	Yes

HP Thin USB powered speakers

Feature	Description
On/Off/Volume controls	Right side of right speaker
Power LED	Front of right speaker (green)
Frequency response	FO to 20 kHz
Watts	2/3 W (normal/maximum)
Dimensions/Speaker (H x W x D)	14.52 x 9.50 x 2.45 cm (5.72 x 3.74 x 0.96 in)
Net weight	0.31 kg (0.68 lbs)
Color	Black
Environmental (all conditions non-condensing)	**Operating temperature:** -10° to 40°C (14° to 104°F) **Relative humidity:** 40% to 90%
Speaker cable length	• Input cord: 1800 mm (5.91 ft) • L-channel cord: 1000 mm (3.28 ft) • USB cord: 1800 mm (5.91 ft)

Environmental specifications

Feature	Description
Eco-Label certifications and declarations	• US ENERGY STAR • IT ECO declaration • EPEAT Gold where HP registers commercial desktop products.
System configuration	• The configuration used for the Energy Consumption and Declared Noise Emissions data for the Small Form Factor Desktop model is based on a typically configured product. • The configuration used for the Energy Consumption and Declared Noise Emissions data for the Microtower Desktop model is based on a typically configured product.
Energy consumption	

Feature	115 V ac	230 V ac	100 V ac
Normal operation	41.77 W	41.64 W	41.67 W
Sleep (Energy Star low power mode)	1.92 W	2.21 W	1.91 W
Off	0.66 W	0.89 W	0.64 W

Heat dissipation

Feature	115 V ac	230 V ac	100 V ac
Normal operation	143 BTU/hr	142 BTU/hr	142 BTU/hr
Sleep	6 BTU/hr	7 BTU/hr	6 BTU/hr
Off	2 BTU/hr	3 BTU/hr	2 BTU/hr

NOTE: Heat dissipation is calculated based on the measured watts, assuming the service level is attained for one hour.

Declared noise emissions (in accordance with ISO 7779 and ISO 9296)

Feature	Sound Power (LWAd, bels)	Sound Pressure (LpAm, decibels)
Idle	3.8	28
Fixed Disk (random writes)	3.9	28

Longevity and upgrading

This product can be upgraded, possibly extending its useful life by several years. Upgradeable features and/or components contained in the product may include:

- Intel LGA775 processor socket
- 8 USB ports
- 2 empty PCI slots (2 low profile or 2 full-height with optional riser)
- 1 empty PCIe x1 slot
- 1 empty PCIe x16 slot
- 1 internal drive slot
- 1 SATA optical drive slot
- 4 memory slots
- 1 serial port (optional)
- 1 external diskette drive (optional)

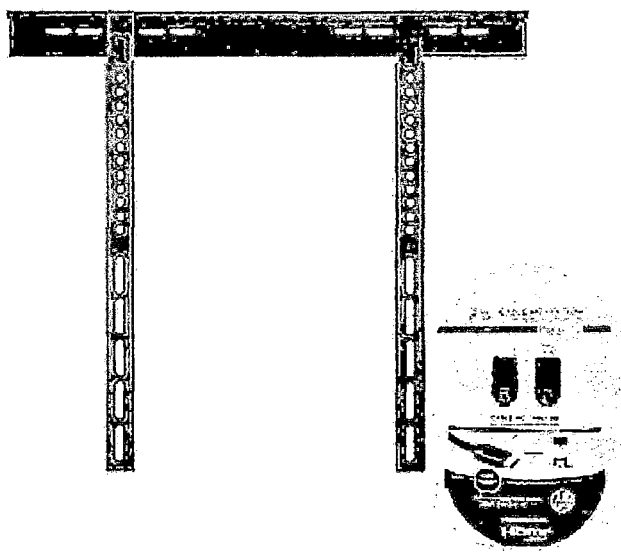
Batteries

This battery(s) in this product comply with EU Directive 2006/66/EC.
Batteries used in the product do not contain:

- Mercury greater the 5 ppm by weight
- Cadmium greater than 10 ppm by weight

Battery size: CR2032 (coin cell)
Battery type: Lithium

Rack Fijo LCD/LED 32" a 55" + HDMI Fujitajapan



Descripción

Rack Fijo LCD/LED 32" a 55" + HDMI

CARACTERÍSTICAS DEL RACK

Para pantallas TV Plasma/LCD
Compatible con TV de 32" a 55"
Soporta un Peso hasta 55 Kg máx.
Distancia de Pared 9mm
Incluye accesorios para fijar a pared

CABLE HDMI

HDMI V1.3 compatibles
Contacto en oro 24k
Cable con escudo triple 100%
Cobre libre de oxígeno
Resolución 1080p

Supresor de Picos Forza

Entrada	
Entrada voltaje nominal:	110/240
Margen de Voltaje:	No
Watts:	1875-2200
Entrada Frecuencia:	50/60Hz
Salida	
Salida Voltaje nominal:	110/240
Salida Frecuencia:	50/60Hz
Número de Tomas:	6

PCEL

Tarjeta de Video ASUS NVIDIA GeForce GT 630, 2 GB GDDR3, HDMI, DVI. Puerto PCI Express 2.0.

Descripción

ASUS GeForce GT630

La nueva ASUS GeForce GT630 (GK208, 64 bits) incorpora 384 núcleos CUDA, una cifra cuatro veces superior a la GPU del diseño de referencia (GF108, 128 bits).

Características

• Ideal para equipos HTPC
El diseño especial de los disipadores permite eliminar los excesos de temperatura mediante un diseño pasivo que resulta totalmente silencioso.

• Mejora la refrigeración y prolonga la vida útil
La aleación que incorporan los componentes a cargo de la alimentación reduce la pérdida energética, mejora la durabilidad y ofrece un funcionamiento con una temperatura más baja. Las bobinas choke eliminan los zumbidos al trabajar a carga plena y los condensadores ofrecen una vida útil de 50 000 horas, 2.5 veces superior a los condensadores tradicionales.

• NVIDIA Adaptive V-Sync
Disfruta del gaming más fluido con las innovaciones para gaming de NVIDIA. Esta tecnología ajusta la sincronía vertical a las FPS actuales para asegurar una acción perfectamente fluida.

• NVIDIA PhysX
Disfruta de explosiones, escombros y personajes más realistas con un cambio de procesamiento físico a gráfico diez veces más rápido, lo que permite el cálculo de más efectos complejos en tiempo real.

Especificaciones

Especificaciones de la Tarjeta de Video

Chipset	NVIDIA
GPU	GeForce GT 630
CUDA Cores	384
Processor Clock (MHz)	902
Memoria	2GB
Tipo de Memoria	GDDR3
Interfaz de Memoria	64 bits
Frecuencia de la Memoria	1600 MHz
DirectX	DirectX 11
OpenGL	OpenGL 4.3
Máxima Resolución DVI	2560 x 1600
Interfaz	PCI Express 2.0
Soporte para Low Profile	-

Salidas de Video

HDMI	1 x HDMI
DVI	1 x DVI
DisplayPort	No incluye
Mini DisplayPort	No incluye
Mini HDMI	No incluye
VGA	1 x VGA

Características Físicas

Dimensiones	137 x 69 x 30 mm

Requerimientos del Sistema

Eléctricos	Fuente de poder de 300 Watts con 20 A en el riel de 12 V

Microsoft®

Wireless Desktop 800

Technical Data Sheet

Version Information	
Product Name	Microsoft® Wireless Desktop 800
Product Version	Microsoft Wireless Desktop 800
Keyboard Version	Microsoft Wireless Keyboard 800
Mouse Version	Microsoft Wireless Mouse 1000
Transceiver Version	Microsoft 2.4 GHz Transceiver v8.0
Product Dimensions	
Keyboard Length	19.1 inches (486 millimeters)
Keyboard Width	8.93 inches (227 millimeters)
Keyboard Depth/Height	1.79 inches (45.7 millimeters)
Keyboard Weight	45.8 ounces (1300 grams) includes 2 AA alkaline batteries: typical battery weight may vary
Mouse Length	4.47 inches (113 millimeters)
Mouse Width	2.29 inches (58.3 millimeters)
Mouse Depth/Height	1.56 inches (39.6 millimeters)
Mouse Weight	2.32 ounces (65.9 grams) includes 2 AA alkaline batteries: typical battery weight may vary
Transceiver Length	1.09 inches (27.6 millimeters)
Transceiver Width	0.59 inches (15.0 millimeters)
Transceiver Depth/Height	0.27 inches (6.89 millimeters)
Transceiver Weight	0.09 ounces (2.8 grams)
Compatibility and Localization	
Interface	USB 2.0 Compatible
Operating Systems[1]	• Microsoft Windows® 8.1, Windows 8, Windows RT 8.1, Windows RT 8, and Windows 7 • Macintosh Mac OS X v10.7-10.9 • Android 3.2 and 4.2 [1]Advanced functionality not available with all devices and/or operating systems. See compatibility information at: microsoft.com/hardware/compatibility.
Top-line System Requirements	Requires a PC that meets the requirements for and has installed one of these operating systems: • Windows 8.1, Windows 8, or Windows 7 • 150 MB • USB
Compatibility Logos	• Compatible with Microsoft Windows 8 and Windows RT • Mac logo
Software Localization	No software required
Keyboard Localization	Available language sets will vary by product and sales channel. **104 key configuration:** Arabic, Chinese (Simplified), Chinese (Traditional), Czech, English (Canada), English (North America), Greek, Hebrew, International English (Euro), International English (ROW), Russian, and Thai **105 key configuration:** All Nordic, English (UK), French (Belgium/Azerty), French (Canada), French (France), German (Germany), German (Switzerland/Luxemburg), Hungarian, Iberian (Portuguese), Italian, Spanish (Euro), Spanish (Latin America), and Turkish **106 key configuration:** Korean **107 key configuration:** Brazilian **109 key configuration:** Japanese
Tracking Technology	
Mouse Tracking System	LED optical technology
Imaging Rate	Dynamically adaptable to 3000 frames per second
X-Y Resolution	1000 points per inch (39.4 points per millimeter)
Tracking Speed	Up to 20 inches (508 millimeters) per second
Wireless Technology	
Wireless Frequency	2.4 GHz frequency range
Wireless Range	15 feet (5 meters) typical. Note: RF range is affected by many factors, such as nearby metallic objects and relative positioning of the mouse and receiver.
Product Feature Performance	
QWERTY Key Life	5,000,000 actuations per key
Hot Key Features	Windows 8 Charms keys, Windows Start key, and Calculator
Hot Key Life	500,000 actuations per key
Media Key Features	Mute, Volume -, Volume +, and Play/Pause
Media Key Life	500,000 actuations per key
Typing Speed	1000 characters per minute
Mouse Button Features	3 buttons including scroll wheel button
Mobility Features	Power switch turns mouse off, conserving battery life
Mouse On/Off Switch Life	4,000 actuations
Right & Left Button Life	3,000,000 actuations at no more than 4 actuations per second
Wheel Button Life	250,000 actuations at no more than 4 actuations per second
Mouse Scrolling Features	Standard vertical scrolling
Wheel Vertical Scrolling Life	• 85,000 revolutions (away from user) • 300,000 revolutions (towards user)
Storage Temperature & Humidity	-40 °F (-40 °C) to 140 °F (60 °C) at < 5% to 65% relative humidity (non-condensing)
Operating Temperature & Humidity	32 °F (0 °C) to 104 °F (40 °C) at <5% to 80% relative humidity (non-condensing)
Power Requirements	
Battery Type and Quantity	• Keyboard: 2 AAA alkaline batteries (included) • Mouse: : 2 AA alkaline batteries (included)
Battery Life	• Keyboard: 15 months typical • Mouse: 8 months typical

Microsoft

Technical Data Sheet

Certification Information		
Country of Manufacture	People's Republic of China (PRC)	
ISO 9001 Qualified Manufacturer	Yes	
ISO 14001 Qualified Manufacturer	Yes	
Restriction on Hazardous Substances	This device complies with all applicable worldwide regulations and restrictions including, but not limited to: EU directive 2002/95/EC on the Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment and EU Registration Evaluation and Authorization of Chemicals (REACH) regulation regarding Substances of Very High Concern.	
FCC/IC ID	This Class B digital apparatus complies with Part 15 of the U.S. Federal Communications Commission (FCC) rules, Canadian ICES-003, and RSS-210. Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. Tested to comply with FCC (U.S. Federal Communications Commission) Standards. For home or office use. The term "IC:" before the certification/registration number only signifies that the Industry Canada technical specifications were met. Model numbers: 1455, Wireless Keyboard 800: 1454, Wireless Mobile Mouse 1000 and 1461, Microsoft 2.4GHz Transceiver v8.0, FCC IDs: C3K1455, C3K1454, and C3K1461.	
Regulacion para México	La operación de este equipo está sujeta a las siguientes dos condiciones: (1) es posible que este equipo o dispositivo no cause interferencia perjudicial y (2) este equipo o dispositivo debe aceptar cualquier interferencia, incluyendo la que pueda causar su operación no deseada.	
Agency and Regulatory Marks	• CNC Certificate (Argentina) • ACA/MED Declaration of Conformity (Australia and New Zealand) • TRA Certificate (Bahrain) • ANATEL Certificate (Brazil) • IC ID, Certificate of Acceptance (Canada) • SUBTEL Certificate (Chile) • CMIT Certificate (China) • EIP Pollution Control Mark, EPUP (China) • Indotel Certificate (Dominican Republic) • R&TTE Declaration of Conformity, Safety and EMC (European Union) • WEEE (European Union) • NTRA Certificate (Egypt) • CONATEL Certificate (Honduras) • ETA Certificate (India) • POSTEL Certificate (Indonesia) • MIC Certificate (Israel) • VCCI and Telec Certificates (Japan) • TRC Certificate (Jordan) • KZ Certificate (Kazakhstan) • CCK Certificate (Kenya) • KCC Certificate (Korea) • MPT Certificate (Kuwait) • MOT Certificate (Lebanon) • SIRIM Certificate (Malaysia)	• ICTA Certificate (Mauritius) • COFETEL Certificate (Mexico) • ANRT Certificate (Morocco) • NCC Certificate (Nigeria) • TRA Certificate (Oman)• PTA Certificate (Pakistan) • MTC Certificate (Peru) • NTC Certificate (Philippines) • ICT Certificate (Qatar) • FAC and GOST Certificates (Russia) • CITC Letter (Kingdom of Saudi Arabia) • RATEL Certificate (Serbia) • IDA Registration (Singapore) • ICASA Certificate (South Africa) • BSMI and NCC Certificates (Taiwan) • SDoC Certificate (Thailand) • CERT Certificate (Tunisia) • UkrSEPRO Certificate (Ukraine) • TRA Certificate (United Arab Emirates) • URSEC Certificate (Uruguay) • FCC ID, Grant of Equipment Authorization (USA) • UL and cUL Listed Accessory (USA and Canada) • CONATEL Certificate (Venezuela) • CB Scheme Certificate (International)
Windows Certification Kit (WCK)	Desktop ID: 1612258 (32-bit) and 1608520 (64-bit) Microsoft Windows 8.1	

ANEXOS

B. Configuración VPN Cliente.

========= Configuración Interfaces ==========

```
/interface ethernet
set [ find default-name=ether1 ] name="Conexion a Internet"
set [ find default-name=ether2 ] name="Conexion a la Red"
/interface pptp-server server
set default-profile="Rimac Profile" enabled=yes
```

========= Configuración VPN CLIENT ==========

```
/ppp profile
add name="Rimac Profile" use-encryption=required
/ppp secret
add local-address=172.172.254.200 name=MRimac password=RIMACVPN \
   profile="Rimac Profile" remote-address=172.172.254.201 service=\
   pptp
```

========= Configuración IP , DNS and Routes ==========

```
/ip address
add address=192.168.10.230/24 interface="Conexion a Internet" \
   network=192.168.10.0
add address=172.172.254.200/24 interface="Conexion a la Red" \
   network=172.172.254.0
/ip dns
set allow-remote-requests=yes servers=200.48.225.130,200.48.225.146


/ip firewall nat
add action=masquerade chain=srcnat src-address=172.172.254.0/24
```

```
/ip route
add distance=1 gateway=192.168.10.1
add distance=1 dst-address=172.172.10.0/24 gateway=172.172.254.1
add distance=1 dst-address=172.172.20.0/24 gateway=172.172.254.1
add distance=1 dst-address=172.172.30.0/24 gateway=172.172.254.1
add distance=1 dst-address=172.172.50.0/24 gateway=172.172.254.1
add distance=1 dst-address=172.172.60.0/24 gateway=172.172.254.1
add distance=1 dst-address=172.172.70.0/24 gateway=172.172.254.1
add distance=1 dst-address=172.172.80.0/24 gateway=172.172.254.1
add distance=1 dst-address=172.172.90.0/24 gateway=172.172.254.1
add distance=1 dst-address=172.172.100.0/24 gateway=172.172.254.1
add distance=1 dst-address=172.172.110.0/24 gateway=172.172.254.1
add distance=1 dst-address=172.172.120.0/24 gateway=172.172.254.1
add distance=1 dst-address=172.172.130.0/24 gateway=172.172.254.1
add distance=1 dst-address=172.172.160.0/24 gateway=172.172.254.1
add distance=1 dst-address=172.172.170.0/24 gateway=172.172.254.1
add distance=1 dst-address=172.172.180.0/24 gateway=172.172.254.1
add distance=1 dst-address=172.192.10.0/24 gateway=172.172.254.1
add distance=1 dst-address=172.192.20.0/24 gateway=172.172.254.1
add distance=1 dst-address=172.192.30.0/24 gateway=172.172.254.1
```

========= Configuración Interfaces ================

```
/interface ethernet
set [ find default-name=ether1 ] name="Conexion a Internet"
set [ find default-name=ether2 ] name="Conexion a la Red"
/interface pptp-server server
set default-profile="MDSL Profile" enabled=yes
```

========= Configuración VPN CLIENT ================

```
/ppp profile
add name=" MDSL Profile" use-encryption=required
/ppp secret
add local-address=172.25.1.200  name=MDSL password=MDSLVPN \
   profile=" MDSL Profile" remote-address=172.25.1.201 service=\
   pptp
```

========= Configuración IP , DNS and Routes ================

```
/ip address
add address=10.10.10.53/24 interface="Conexion a Internet" \
   network=10.10.10.0
add address=172.25.1.200/24 interface="Conexion a la Red" \
   network=172.25.1.0
/ip dns
set allow-remote-requests=yes servers=200.48.225.130,200.48.225.146

/ip firewall nat
add action=masquerade chain=srcnat src-address=172.25.1.0/24
```

```
/ip route
add distance=1 gateway=10.10.10.1
add distance=1 dst-address=172.27.2.0/24 gateway=172.25.1.1
add distance=1 dst-address=172.27.3.0/24 gateway=172.25.1.1
add distance=1 dst-address=172.27.4.0/24 gateway=172.25.1.1
add distance=1 dst-address=172.27.5.0/24 gateway=172.25.1.1
add distance=1 dst-address=172.25.1.0/24 gateway=172.25.1.1
add distance=1 dst-address=172.25.2.0/24 gateway=172.25.1.1
add distance=1 dst-address=172.25.3.0/24 gateway=172.25.1.1
add distance=1 dst-address=172.25.4.0/24 gateway=172.25.1.1
add distance=1 dst-address=172.25.5.0/24 gateway=172.25.1.1
add distance=1 dst-address=172.25.6.0/24 gateway=172.25.1.1
add distance=1 dst-address=172.26.1.0/24 gateway=172.25.1.1
add distance=1 dst-address=172.26.2.0/24 gateway=172.25.1.1
add distance=1 dst-address=172.26.3.0/24 gateway=172.25.1.1
add distance=1 dst-address=172.26.4.0/24 gateway=172.25.1.1
add distance=1 dst-address=172.20.200.0/24 gateway=172.25.1.1
add distance=1 dst-address=172.20.100.0/24 gateway=172.25.1.1
```

========= Configuración Interfaces ==========

```
/interface ethernet
set [ find default-name=ether1 ] name="Conexion a Internet"
set [ find default-name=ether2 ] name="Conexion a la Red"
/interface pptp-server server
set default-profile="MCuzco Profile" enabled=yes
```

========= Configuración VPN CLIENT ==========

```
/ppp profile
add name=" MCuzco Profile" use-encryption=required
/ppp secret
add local-address=10.10.101.200  name=MCuzco password=McuzcoVPN\
   profile=" MCuzco Profile" remote-address=10.10.101.201 service=\
   pptp
```

========= Configuración IP , DNS and Routes ==========

```
/ip address
add address=172.172.10.20/24 interface="Conexion a Internet" \
   network=172.172.10.0
add address=10.10.101.200/24 interface="Conexion a la Red" \
   network=10.10.101.0
/ip dns
set allow-remote-requests=yes servers=200.48.225.130,200.48.225.146

/ip firewall nat
add action=masquerade chain=srcnat src-address=10.10.101.0/24
```

```
/ip route
add distance=1 gateway=172.172.10.1
add distance=1 dst-address=20.20.100.0/24 gateway=10.10.101.1
add distance=1 dst-address=20.20.101.0/24 gateway=10.10.101.1
add distance=1 dst-address=20.20.102.0/24 gateway=10.10.101.1
add distance=1 dst-address=20.20.103.0/24 gateway=10.10.101.1
add distance=1 dst-address=20.20.104.0/24 gateway=10.10.101.1
add distance=1 dst-address=20.20.105.0/24 gateway=10.10.101.1
add distance=1 dst-address=20.20.106.0/24 gateway=10.10.101.1
add distance=1 dst-address=20.20.108.0/24 gateway=10.10.101.1
add distance=1 dst-address=20.20.109.0/24 gateway=10.10.101.1
add distance=1 dst-address=10.10.100.0/24 gateway=10.10.101.1
add distance=1 dst-address=10.10.101.0/24 gateway=10.10.101.1
add distance=1 dst-address=10.10.102.0/24 gateway=10.10.101.1
add distance=1 dst-address=10.10.103.0/24 gateway=10.10.101.1
add distance=1 dst-address=10.10.104.0/24 gateway=10.10.101.1
add distance=1 dst-address=10.10.105.0/24 gateway=10.10.101.1
add distance=1 dst-address=10.10.106.0/24 gateway=10.10.101.1
add distance=1 dst-address=10.10.108.0/24 gateway=10.10.101.1
add distance=1 dst-address=172.192.40.0/24 gateway=10.10.101.1
```

========= Configuración Interfaces ==========

```
/interface ethernet
set [ find default-name=ether1 ] name="Conexion a Internet"
set [ find default-name=ether2 ] name="Conexion a la Red"
/interface pptp-server server
set default-profile="MPiura Profile" enabled=yes
```

========= Configuración VPN CLIENT ==========

```
/ppp profile
add name=" MPiura Profile" use-encryption=required
/ppp secret
add local-address=172.26.1.200  name=MPiura password=MPiuraVPN\
   profile=" MPiura Profile" remote-address=172.26.1.201 service=\
   pptp
```

========= Configuración IP , DNS and Routes ==========

```
/ip address
add address=172.28.1.160/24 interface="Conexion a Internet" \
   network=172.28.1.0
add address=172.26.1.200/24 interface="Conexion a la Red" \
   network=172.26.1.0
/ip dns
set allow-remote-requests=yes servers=200.48.225.130,200.48.225.146

/ip firewall nat
add action=masquerade chain=srcnat src-address=172.26.1.0/24
```

```
/ip route
add distance=1 gateway=172.28.1.1
add distance=1 dst-address=172.24.1.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.24.2.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.24.3.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.24.4.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.24.5.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.24.6.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.23.1.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.23.2.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.23.3.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.23.4.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.23.5.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.23.6.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.23.7.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.23.8.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.23.9.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.23.10.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.21.1.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.21.2.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.21.3.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.21.4.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.21.5.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.21.6.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.21.7.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.25.6.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.25.7.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.25.8.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.25.10.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.25.11.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.25.12.0/24 gateway=172.26.1.1
```

```
add distance=1 dst-address=172.25.13.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.25.14.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.22.1.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.22.2.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.22.3.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.22.4.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.22.5.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.22.6.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.26.5.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.26.6.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.26.7.0/24 gateway=172.26.1.1
add distance=1 dst-address=172.26.8.0/24 gateway=172.26.1.1
```

MUNICIPALIDAD DISTRITAL DE CASTILLA

========= Configuración Interfaces ==========

```
/interface ethernet
set [ find default-name=ether1 ] name="Conexion a Internet"
set [ find default-name=ether2 ] name="Conexion a la Red"
/interface pptp-server server
set default-profile="MCastilla Profile" enabled=yes
```

========= Configuración VPN CLIENT ==========

```
/ppp profile
add name=" MCastilla Profile" use-encryption=required
/ppp secret
add local-address=172.100.21.200  name=MCastilla password=MCastillaVPN\
   profile=" MCastilla Profile" remote-address=172.100.21.201 service=\
   pptp
```

========= Configuración IP , DNS and Routes ==========

```
/ip address
add address=192.168.1.200/24 interface="Conexion a Internet" \
   network=192.168.1.0
add address=172.100.21.200/24 interface="Conexion a la Red" \
   network=172.100.21.0
/ip dns
set allow-remote-requests=yes servers=200.48.225.130,200.48.225.146

/ip firewall nat
add action=masquerade chain=srcnat src-address=172.100.21.0/24


/ip route
```

```
add distance=1 gateway=192.168.1.1
add distance=1 dst-address=192.100.4.0/24 gateway=172.100.21.200
add distance=1 dst-address=192.100.12.0/24 gateway=172.100.21.200
add distance=1 dst-address=192.100.14.0/24 gateway=172.100.21.200
add distance=1 dst-address=192.100.15.0/24 gateway=172.100.21.200
add distance=1 dst-address=192.100.16.0/24 gateway=172.100.21.200
add distance=1 dst-address=192.100.1.0/24 gateway=172.100.21.200
add distance=1 dst-address=192.100.3.0/24 gateway=172.100.21.200
add distance=1 dst-address=192.100.9.0/24 gateway=172.100.21.200
add distance=1 dst-address=192.100.11.0/24 gateway=172.100.21.200
add distance=1 dst-address=192.100.8.0/24 gateway=172.100.21.200
add distance=1 dst-address=192.100.13.0/24 gateway=172.100.21.200
add distance=1 dst-address=192.100.10.0/24 gateway=172.100.21.200
add distance=1 dst-address=192.100.2.0/24 gateway=172.100.21.200
add distance=1 dst-address=192.100.22.0/24 gateway=172.100.21.200
add distance=1 dst-address=192.100.6.0/24 gateway=172.100.21.200
add distance=1 dst-address=192.100.7.0/24 gateway=172.100.21.200
add distance=1 dst-address=192.100.5.0/24 gateway=172.100.21.200
add distance=1 dst-address=192.100.17.0/24 gateway=172.100.21.200
add distance=1 dst-address=192.100.18.0/24 gateway=172.100.21.200
add distance=1 dst-address=192.100.19.0/24 gateway=172.100.21.200
add distance=1 dst-address=192.100.20.0/24 gateway=172.100.21.200
add distance=1 dst-address=172.100.31.0/24 gateway=172.100.21.200
add distance=1 dst-address=172.100.32.0/24 gateway=172.100.21.200
add distance=1 dst-address=172.100.33.0/24 gateway=172.100.21.200
```

ANEXOS

C. Configuración VPN Servidor.

CONFIGURACION VPN SERVER

X.X.X.X = IPS PUBLICAS DE LAS ENTIDADES

```
/interface ethernet
set [ find default-name=ether1 ] name="Conexion a Internet"
set [ find default-name=ether2 ] name="Salida a Servidor The Dude"
/interface pptp-client
add connect-to=X.X.X.X disabled=no mrru=1600 name="Municipalidad Rimac" \
   password=RIMACVPN user=MRimac
add connect-to=X.X.X.X disabled=no mrru=1600 name="Municipalidad de Castilla" \
   password=MCastillaVPN user=MCastilla
add connect-to=X.X.X.X disabled=no mrru=1600 name="Municipalidad de Piura" \
   password=MPiuraVPN user=MPiura
add connect-to=X.X.X.X disabled=no mrru=1600 name=\
   "Municipalidad de San Juan de Lurigancho" password=MDSLVPN user=MDSL
add connect-to=X.X.X.X disabled=no mrru=1600 name="Municipalidad del Cuzco" \
   password=McuzcoVPN user=MCuzco
/ip address
add address=172.29.20.50/24 interface="Conexion a Internet" network=\
   172.29.20.0
add address=172.200.1.1/24 interface="Salida a Servidor The Dude" network=\
   172.200.1.0
/ip dhcp-server
add address-pool=dhcp_pool1 disabled=no interface=\
   "Salida a Servidor The Dude" lease-time=3d name=dhcp1
/ip dhcp-server network
add address=172.200.1.0/24 gateway=172.200.1.1
/ip dns
set allow-remote-requests=yes servers=200.48.225.130,200.48.225.146
/ip firewall nat
add action=masquerade chain=srcnat src-address=172.200.1.0/24
/ip routeadd distance=1 gateway=172.29.20.1
```

ANEXOS

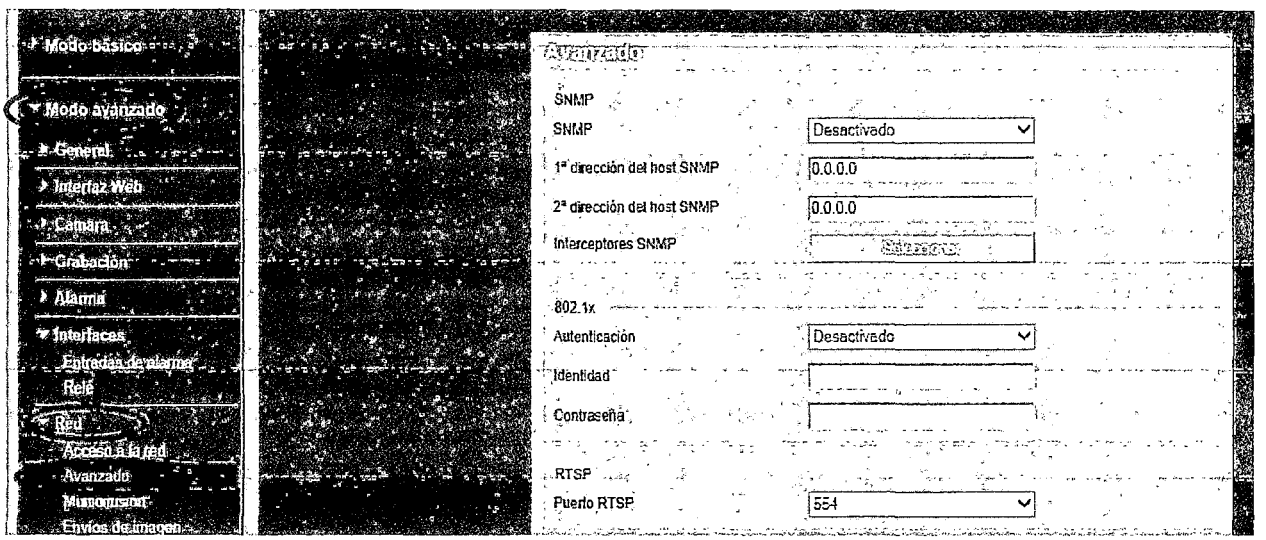
D. Habilitación del Protocolo SNMP.

Habilitación del Protocolo SNMP en los Elementos de Red

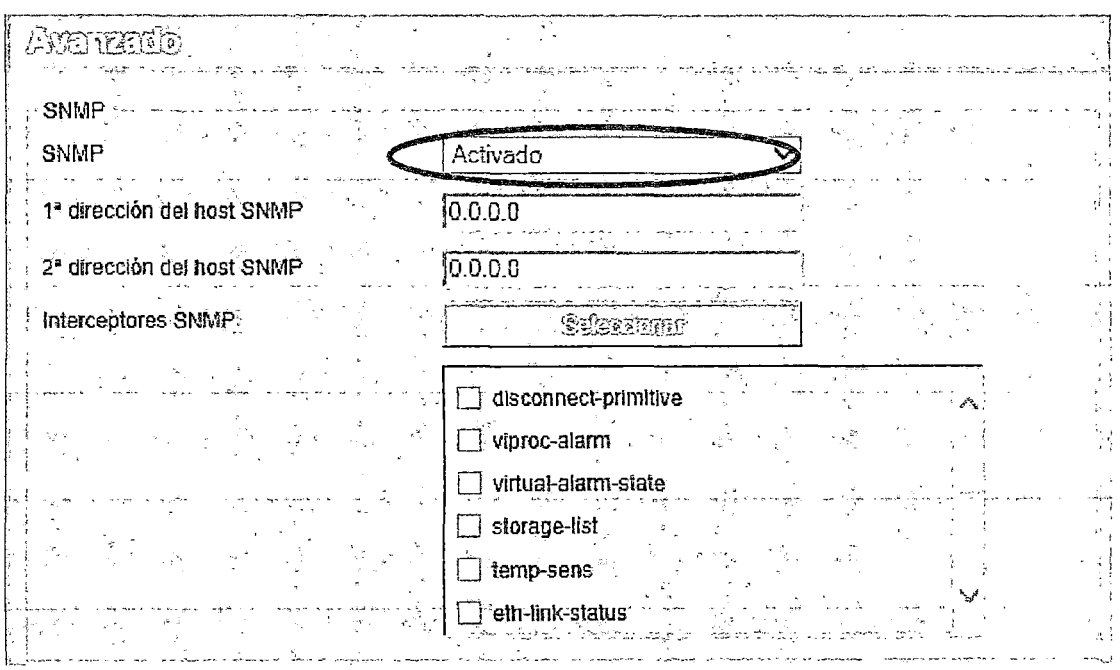
Los dispositivos admite el protocolo SNMP (Protocolo simple de gestión de red) para gestionar y controlar los componentes de red. La unidad es compatible con SNMP MIB II en el código unificado.

A. Habilitación del Protocolo SNMP en las Cámaras Domo PTZ

Para activar el protocolo SNMP, hay que ingresar a Ajustes, en el Modo Avanzado, ir a la pestaña Red > Avanzado.

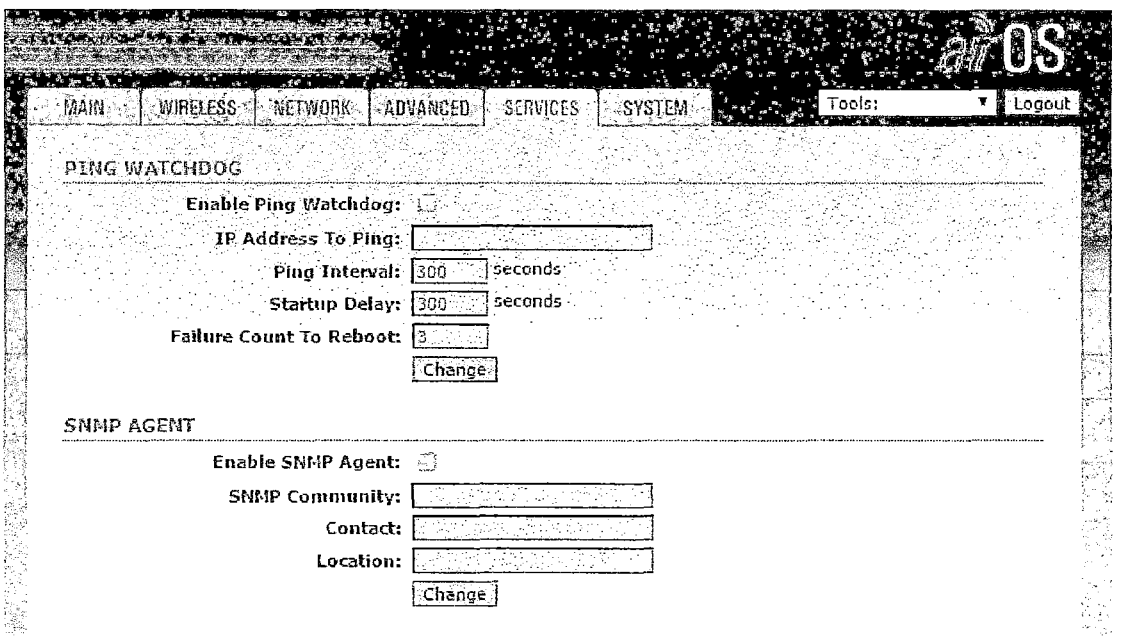


En la opción SNMP seleccionar Activado y Listo.

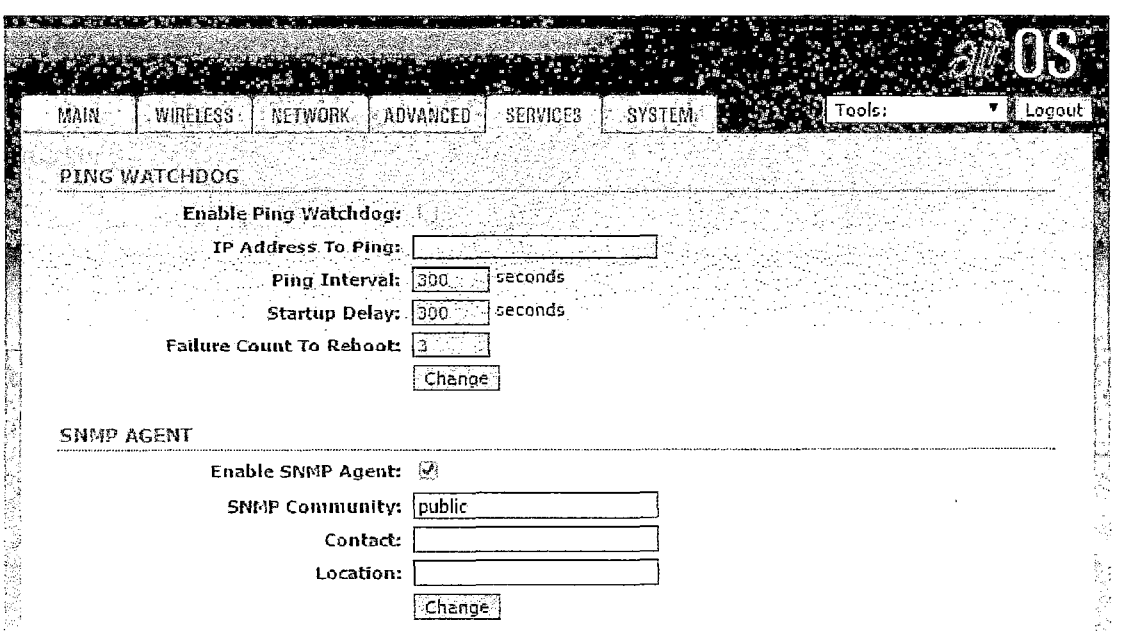


B. Habilitación del Protocolo SNMP en los AP Ubiquiti

Para activar el protocolo SNMP, hay que ingresar a la pestaña Services> SNMP AGENT

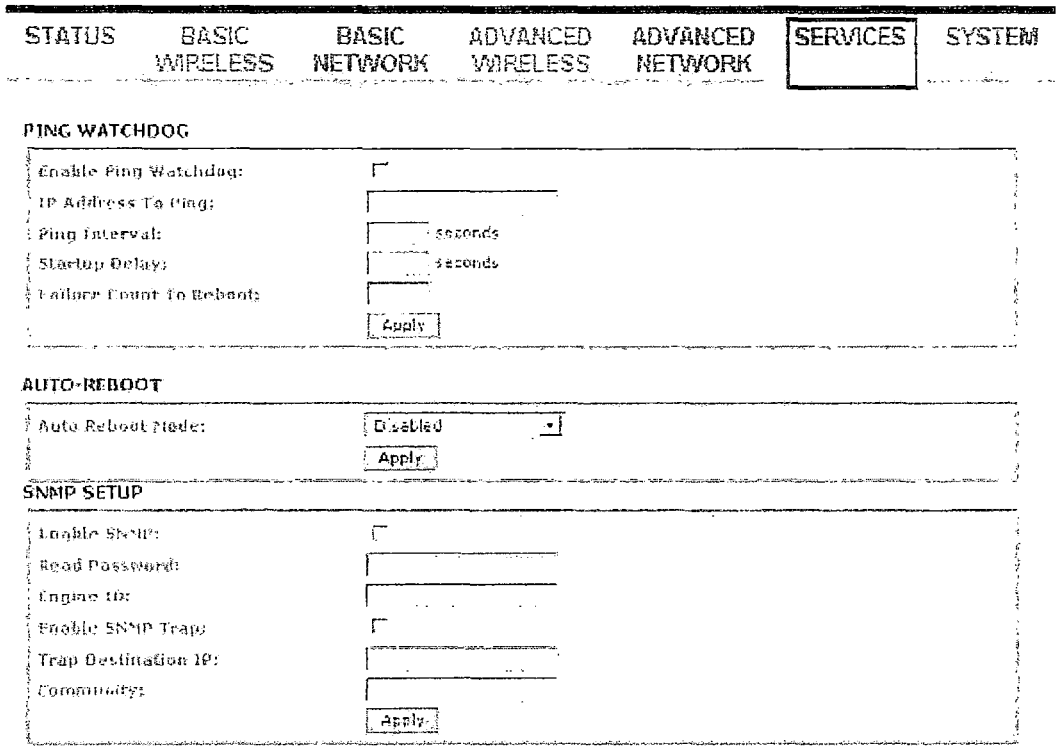


En la opción Enable SNMP Agent habilitar con un check y en SNMP Community, ingresar la comunidad con la que se va a trabajar

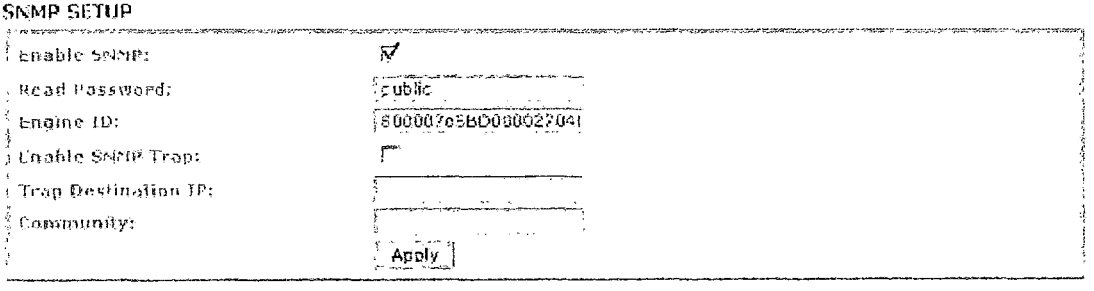


C. Habilitación del Protocolo SNMP en los AP AirNet

Para activar el protocolo SNMP, hay que ingresar a la pestaña Services> SNMP SETUP

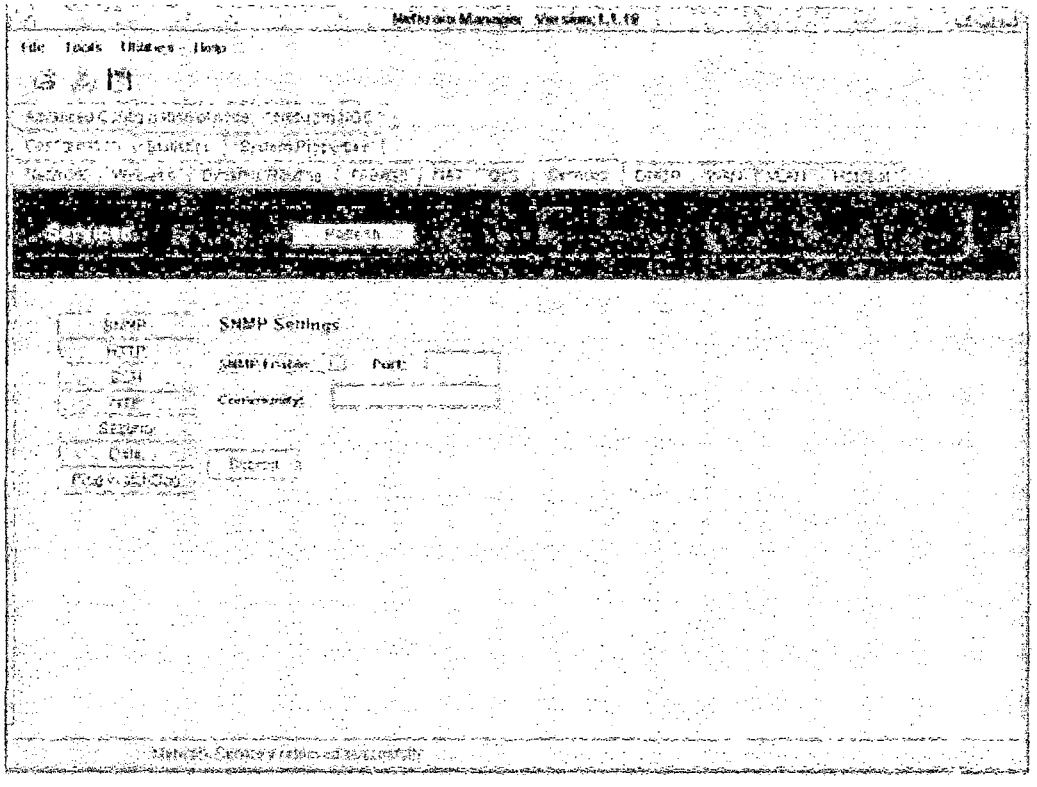


En la opción Enable SNMP habilitar con un check y en Read Password, ingresar la comunidad con la que se va a trabajar, el Engine ID por defecto es el siguiente 800007e5BD00002704D000007c

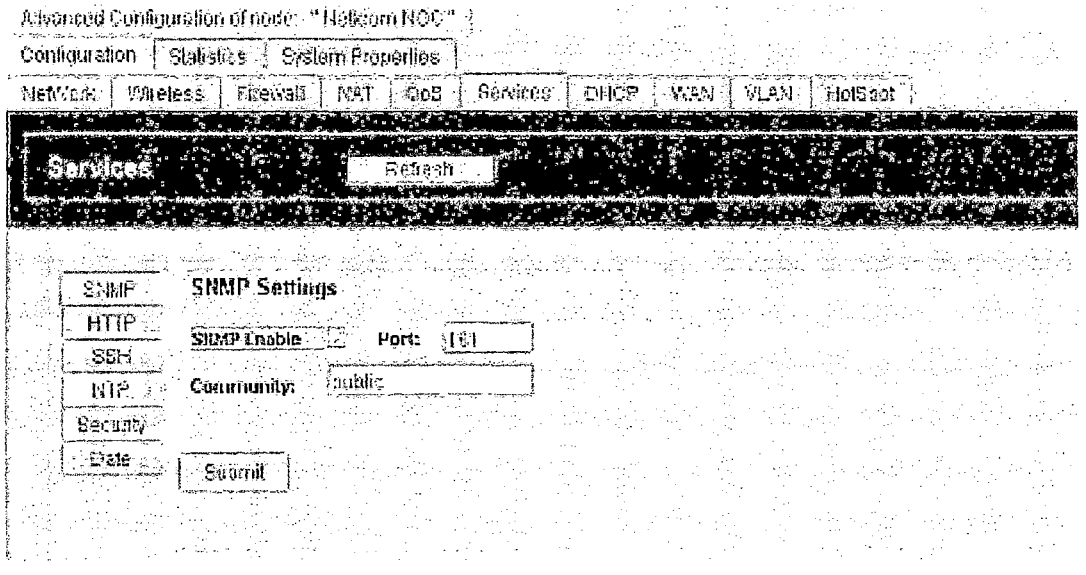


D. Habilitación del Protocolo SNMP en los AP MB-ROMBV4

Para activar el protocolo SNMP, hay que ingresar a Advanced Configuration of Node, ir a la pestaña Configuration > Service.



En la opción SNMP Enable habilitar con un check, ingresar en Port, el port del protocolo 161 y en Community, ingresar la comunidad con la que se va a trabajar



E. Habilitación del Protocolo SNMP en los Routers Mikrotik

Para activar el protocolo SNMP, hay que ingresar el siguiente código:
[admin@MikroTik] > /snmp
[admin@MikroTik] /snmp> set enabled=yes

```
  MMM      MMM       KKK                          TTTTTTTTTTT      KKK
  MMMM    MMMM       KKK                          TTTTTTTTTTT      KKK
  MMM MMMM MMM  III  KKK  KKK  RRRRRR     OOOOOO      TTT     III  KKK  KKK
  MMM  MM  MMM  III  KKKKK     RRR  RRR  OOO  OOO     TTT     III  KKKKK
  MMM      MMM  III  KKK KKK   RRRRRR    OOO  OOO     TTT     III  KKK KKK
  MMM      MMM  III  KKK  KKK  RRR  RRR   OOOOOO      TTT     III  KKK  KKK

  MikroTik RouterOS 6.27 (c) 1999-2015       http://www.mikrotik.com/

[?]             Gives the list of available commands
command [?]     Gives help on the command and list of arguments

[Tab]           Completes the command/word. If the input is ambiguous,
                a second [Tab] gives possible options

/               Move up to base level
..              Move up one level
/command        Use command at the base level
[admin@MikroTik] > /snmp
[admin@MikroTik] /snmp> set enabled=yes
```

Para Comprobar la habilitación ingresamos el comando print

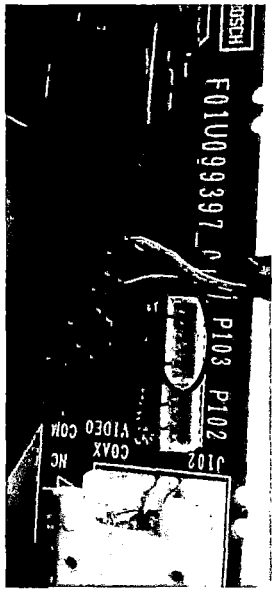
```
Terminal
  MikroTik RouterOS 6.27 (c) 1999-2015       http://www.mikrotik.com/

[?]             Gives the list of available commands
command [?]     Gives help on the command and list of arguments

[Tab]           Completes the command/word. If the input is ambiguous,
                a second [Tab] gives possible options

/               Move up to base level
..              Move up one level
/command        Use command at the base level
[admin@MikroTik] > /snmp
[admin@MikroTik] /snmp> set enabled=yes
[admin@MikroTik] /snmp>
[admin@MikroTik] /snmp> print
           enabled: yes
           contact:
          location:
         engine-id:
       trap-target:
    trap-community: public
      trap-version: 1
  trap-generators:
[admin@MikroTik] /snmp>
```

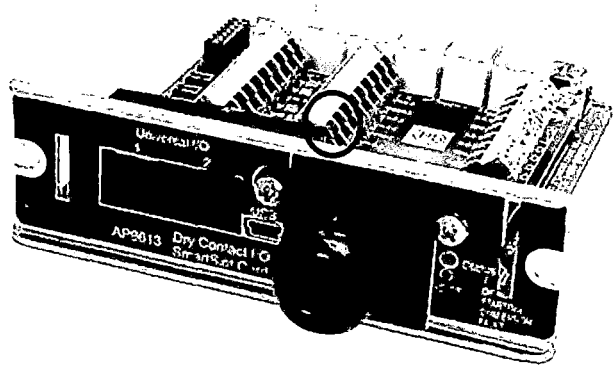
ANEXOS

E. Obtención del Suministro Eléctrico.

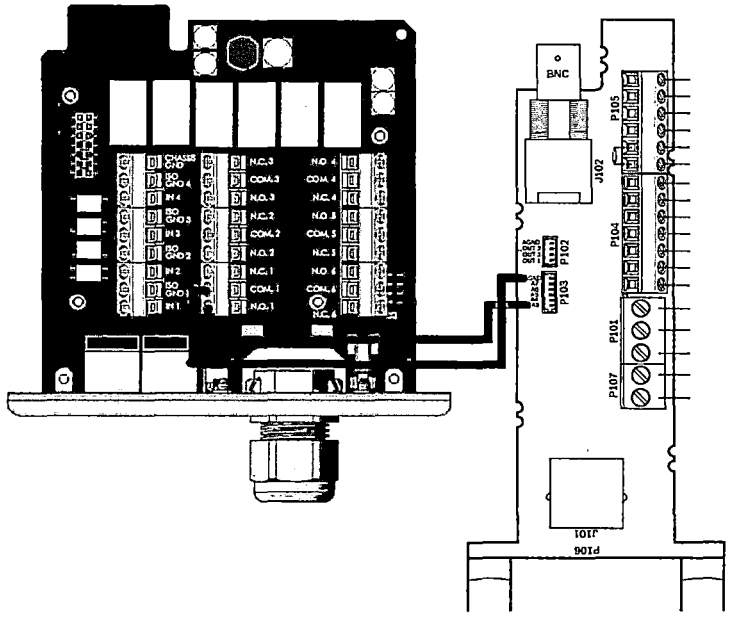
Obtención de la Alarma de Suministro Eléctrico

Para lograr la obtención de la información de corte de energía, en el UPS usamos el Contacto Seco NO 1, y las entradas de alarma 1 de la cámara



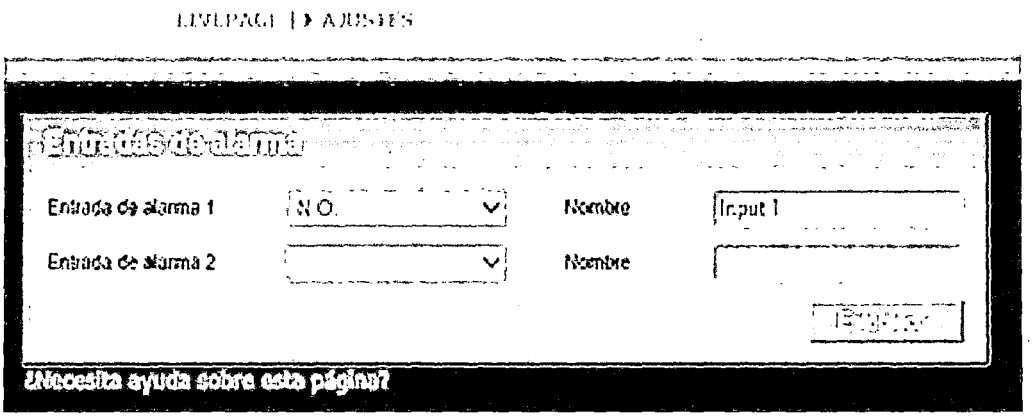


Se configura los Dip Switches del UPS en OFF, OFF, OFF, ON, con esta configuración el contacto se cierra cuando el UPS entra en actividad por corte del suministro eléctrico, este se conecta a la Entrada de Alarma 1, tal como se muestra la siguiente figura



Ya teniendo el hardware conectado, configuramos la entrada 1 de alarma de la cámara como N.O, para que cuando el contacto cierre se encienda la alarma. Para ello vamos a Ajustes> Modo Avanzado y en la pestaña Interfaces elegimos Entradas de Alarma.

En la entrada de Alarma 1 Seleccionamos N.O, y le ponemos un nombre como ejemplo Input 1



Luego Configuramos esta alarma para ser un Traps y así se envíe hacia nuestro servidor a través del protocolo SNMP, esto es necesario para poder visualizar la alarma desde nuestro sistema de monitoreo. Para ello vamos a Ajustes> Modo Avanzado y en la pestaña Red elegimos avanzado.

Activamos el SNMP e indicamos la IP de nuestro servidor y seleccionamos con un check que se envíen el estado de las alarmas virtuales (virtual-alarm-state). Con ello iniciamos el envío de Traps por corte de energía.